

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hirofumi MURATANI, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: ENCRYPTION APPARATUS, DECRYPTION APPARATUS, EXPANDED KEY GENERATING APPARATUS AND METHOD THEREFOR, AND RECORDING MEDIUM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-211686	July 12, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913



22850



日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1011 U.S. PTO
09/902696
07/12/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 7月12日

出 願 番 号

Application Number:

特願2000-211686

出 願 人

Applicant(s):

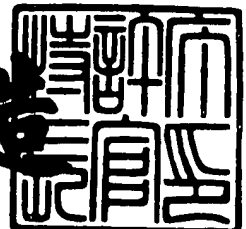
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月11日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 A000003685

【提出日】 平成12年 7月12日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記録媒体

【請求項の数】 18

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

 【氏名】 村谷 博文

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

 【氏名】 本山 雅彦

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

 【氏名】 大熊 建司

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中事業所内

 【氏名】 佐野 文彦

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

 【氏名】 川村 信一

【特許出願人】

 【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記録媒体

【特許請求の範囲】

【請求項 1】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するラウンド処理手段と、

前記ラウンド処理手段の全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するための出力手段とを備え、

前記ラウンド処理手段は、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すものであることを特徴とする暗号化装置。

【請求項 2】

前記ラウンド関数系列は、初段からの段数と最終段からの段数とが一致する 2 つのラウンド関数を互いに逆関数になるように設定したものであることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 3】

前記ラウンド関数系列は、少なくとも第 1 の特定の段と第 2 の特定の段との間の連続する複数段について、該第 1 の特定の段からの段数と該第 2 の特定の段からの段数とが一致する 2 つのラウンド関数を互いに逆関数になるように設定した部分系列を含むものであることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 4】

前記ラウンド関数系列は、少なくとも第 1 の特定の段から段数増加方向へ特定段数隔てた段までの連続する範囲と第 2 の特定の段から段数減少方向へ特定段数隔てた段までの連続する範囲について、該第 1 の特定の段からの段数と該第 2 の特定の段からの段数とが一致する 2 つのラウンド関数を互いに逆関数になるように設定した部分系列を含むものであることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 5】

前記ラウンド関数系列を、請求項 3 または 4 に記載の部分系列を含まないように設定したことを特徴とする請求項 1 に記載の暗号化装置。

【請求項 6】

前記出力手段は、前記拡大鍵の出力のために前記中間状態を用いる際に、該中間状態については、その全ビットのうちから選択した当該中間状態を一意に決定するには十分ではない部分のみを用いることを特徴とする請求項 1 ないし 5 のいずれか 1 項に記載の暗号化装置。

【請求項 7】

前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段若しくは初段から段数増加方向へ所定段数隔てた段までの連続する範囲、及び又は最終段若しくは最終段から段数減少方向へ所定段数隔てた段までの連続する範囲に属するラウンド関数に対応する中間状態は、前記拡大鍵として又はそのもととなるデータとして用いないことを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載の暗号化装置。

【請求項 8】

前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段からの段数と最終段からの段数とが一致する 2 つのラウンド関数に対応する中間状態のいずれか一方又は両方は、前記拡大鍵として又はそのもととなるデータとして用いないことを特徴とする請求項 1 ないし 7 のいずれか 1 項に記載の暗号化装置。

【請求項 9】

前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段若

しくは初段から段数増加方向へ所定段数隔てた段までの連続する範囲、及び又は最終段若しくは最終段から段数減少方向へ所定段数隔てた段までの連続する範囲に属するラウンド関数に対応する中間状態のうち、初段からの段数と最終段からの段数とが一致する2つのラウンド関数のいずれか一方又は両方に対応する中間状態は、前記拡大鍵として又はそのもととなるデータとして用いないことを特徴とする請求項1ないし6のいずれか1項に記載の暗号化装置。

【請求項10】

複数の前記拡大鍵のうちの任意のものが常には一致しないようにしたことを特徴とする請求項1ないし9のいずれか1項に記載の暗号化装置。

【請求項11】

複数の前記拡大鍵のうちの任意のものが、それら拡大鍵の全ビットのうちの任意のビット群についても、常には一致しないようにしたことを特徴とする請求項10に記載の暗号化装置。

【請求項12】

前記ラウンド処理手段及び前記出力手段は、前記データ攪拌処理に必要な拡大鍵数を越える数の拡大鍵を、該データ攪拌処理に提供可能であり、

前記提供可能な拡大鍵のうち実際に前記データ攪拌処理に提供すべき拡大鍵を示す情報、又は前記データ攪拌処理に提供すべき拡大鍵及びその提供する順番を示す情報を拡張共通鍵とし、

前記出力手段は、前記拡張共通鍵に従って、前記拡大鍵を出力することを特徴とする請求項1ないし11のいずれか1項に記載の暗号化装置。

【請求項13】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による復号装置であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するラウンド処理手段と、

前記ラウンド処理手段の全部又は一部の段にて生成された前記中間状態の各々

について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するための出力手段とを備え、

前記ラウンド処理手段は、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すものであることを特徴とする復号装置。

【請求項 1 4】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置又は復号装置に用いられる拡大鍵生成装置であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するラウンド処理手段と、

前記ラウンド処理手段の全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するための出力手段とを備え、

前記ラウンド処理手段は、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すものであることを特徴とする拡大鍵生成装置。

【請求項 1 5】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置のための拡大鍵生成方法であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状

態を入力として所定のラウンド関数を施して新たな中間状態を生成するとともに

全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するステップを有し、

前記中間状態の生成にあたっては、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すことを特徴とする拡大鍵生成方法。

【請求項 1 6】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による復号装置のための拡大鍵生成方法であって

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するとともに

全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するステップを有し、

前記中間状態の生成にあたっては、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すことを特徴とする拡大鍵生成方法。

【請求項 1 7】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置のための拡大鍵生成プログラム

を記録したコンピュータ読取り可能な記録媒体であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するとともに、全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力させ、

前記中間状態の生成にあたっては、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項 1 8】

暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による復号装置のための拡大鍵生成プログラムを記録したコンピュータ読取り可能な記録媒体であって、

複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2 段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するとともに、全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力させ、

前記中間状態の生成にあたっては、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号化時と復号時とで複数の拡大鍵を逆の順番で用いる暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記録媒体に関する。

【0002】

【従来の技術】

電子化された情報、とりわけ著作権に係る情報や機密情報やプライバシーに係る情報等のセキュリティ・コントロールのために、暗号技術の重要性が非常に高くなっている。実際に暗号技術は様々な分野において様々な形で利用されている。

【0003】

暗号方式には様々なものがあるが、そのうちの一つに、共通鍵暗号方式がある。共通鍵暗号方式は、暗号化の際に用いられた鍵と同一の鍵（共通鍵、秘密鍵）を用いて復号が行われる方式である。

【0004】

共通鍵暗号方式にも種々のものがあるが、そのうちの一つに、拡大鍵を用いる方式がある。この方式では、共通鍵をもとに、それが持つビット数より多い総ビット数の複数の拡大鍵を生成する。

【0005】

拡大鍵の生成方式の一つに、共通鍵に対してラウンド関数（段関数）を作用させ、その出力値をもとに拡大鍵を生成するとともに、さらに該出力値にラウンド関数を作用させ、その出力値をもとに次の拡大鍵を生成するとともに、さらに該出力値にラウンド関数を作用させ…、というように、次々とラウンド関数を作用させて拡大鍵を逐次的に生成していくものがある。このような方式をここではラウンド方式と呼ぶものとする。

【0006】

なお、このような拡大鍵生成方式をとる共通鍵暗号方式としては、例えば、共通鍵ブロック暗号方式がある。なお、共通鍵ブロック暗号方式は、データ攪拌部

についても、処理単位となる所定ビット長のブロック・データに、ラウンド関数を次々と作用させて暗号化または復号を行う構造を有するものであり、その代表的な基本構造に S P N 型と F e i s t e l 型等がある。

【 0 0 0 7 】

さて、拡大鍵の生成にラウンド方式をとる場合には、例えばブロック暗号のように、暗号化の際に用いられた順番とは逆の順番で拡大鍵を用いることが要求される。

【 0 0 0 8 】

以下、このような方式の問題点について説明する。

【 0 0 0 9 】

図 3 8 に、従来の暗号化装置の拡大鍵生成部の構成例を示す。

【 0 0 1 0 】

まず、データ攪拌部では暗号化処理に拡大鍵（1）を必要とする。そこで、共通鍵にラウンド関数（1）を作用させ、その出力値を求め、これに拡大鍵変換（1）を作用させて、拡大鍵（1）を得る。データ攪拌部は、この拡大鍵（1）を用いて暗号化処理を行う。

【 0 0 1 1 】

次に、データ攪拌部では暗号化処理に拡大鍵（2）を必要とする。そこで、ラウンド関数（1）の出力値にラウンド関数（2）を作用させ、その出力値を求め、これに拡大鍵変換（2）を作用させて、拡大鍵（2）を得る。データ攪拌部は、この拡大鍵（2）を用いて暗号化処理を行う。

【 0 0 1 2 】

以降、同様にして、拡大鍵生成部による拡大鍵の生成と、データ攪拌部による暗号化処理が行われる。

【 0 0 1 3 】

ここで、復号時の処理を考える。

【 0 0 1 4 】

復号時には、暗号時とは逆の順、すなわち、拡大鍵（n）→拡大鍵（1）の順番に、拡大鍵を用いる必要がある。ところが、図 3 8 と同様の構成の拡大鍵生成

部を有する従来の復号装置では、拡大鍵は、拡大鍵（１）→拡大鍵（ｎ）の順に生成されるので、例えば、データ攪拌部の処理に先立って、すべての拡大鍵を生成し、メモリに記憶しておく必要があった。

【 0 0 1 5 】

しかしながら、例えばＩＣカードのように貧弱なハードウェア環境しかない装置では、復号に必要な拡大鍵をすべて格納するだけの記憶領域の余裕がないという問題点がある。

【 0 0 1 6 】

一方、この問題を回避するために、図 3 9 に例示するような構成が考えられる。この従来の復号装置の拡大鍵生成部の構成例では、一旦、暗号化時と同一の拡大鍵生成処理を行って最終ラウンドでラウンド関数を作用させて得られる出力値（１０２０）を求める。その後、あらためて、該出力値（１０２０）に暗号化時とは逆のラウンド方向に各ラウンド関数の逆関数を作用させて、拡大鍵（ｎ）→拡大鍵（１）の順に、すなわち *On-the-fly* に拡大鍵を生成していく。

【 0 0 1 7 】

しかしながら、最初に暗号化時と同一の拡大鍵生成処理を行う不要な時間のために、復号が開始されるまでの遅延時間が発生するという問題点があった。

【 0 0 1 8 】

【発明が解決しようとする課題】

以上説明したように、従来の技術では、拡大鍵を逆順に生成することはできないので、復号処理に先立って、全拡大鍵を生成し記憶しておく必要があるが、例えばＩＣカードのように貧弱なハードウェア環境では、復号に必要な拡大鍵をすべて格納するだけの記憶領域の余裕がないという問題点があった。

【 0 0 1 9 】

また、*On-the-fly* の鍵生成によって、この問題を回避するためには、一旦、暗号化時と同一の拡大鍵生成処理を行って最終ラウンドでラウンド関数を作用させて得られる出力値を求めた後に、あらためて該出力値に逆のラウンド方向に各ラウンド関数の逆関数を作用させていくことが必要になるが、この場合も、復号が開始されるまでの遅延時間が避けられないという問題点があった。

【 0 0 2 0 】

本発明は、上記事情を考慮してなされたもので、拡大鍵生成のための遅延時間の発生を回避しもしくは小さくし、かつ、*One-time-only*の鍵生成を可能とした暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記録媒体を提供することを目的とする。

【 0 0 2 1 】

【課題を解決するための手段】

本発明は、暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置または復号装置であって、複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するラウンド処理手段と、前記ラウンド処理手段の全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するための出力手段とを備え、前記ラウンド処理手段は、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すものであることを特徴とする。

【 0 0 2 2 】

好ましくは、前記ラウンド関数系列は、初段からの段数と最終段からの段数とが一致する2つのラウンド関数を互いに逆関数になるように設定したものであるようにしてもよい。また、好ましくは、前記ラウンド関数系列は、少なくとも第1の特定の段と第2の特定の段との間の連続する複数段について、該第1の特定の段からの段数と該第2の特定の段からの段数とが一致する2つのラウンド関数を互いに逆関数になるように設定した部分系列を含むものであるようにしてもよい。また、好ましくは、前記ラウンド関数系列は、少なくとも第1の特定の段から段数増加方向へ特定段数隔てた段までの連続する範囲と第2の特定の段から段

数減少方向へ特定段数隔てた段までの連続する範囲について、該第 1 の特定の段からの段数と該第 2 の特定の段からの段数とが一致する 2 つのラウンド関数を互いに逆関数になるように設定した部分系列を含むものであるようにしてもよい。

【 0 0 2 3 】

好ましくは、前記出力手段は、前記拡大鍵の出力のために前記中間状態を用いる際に、該中間状態については、その全ビットのうちから選択した当該中間状態を一意に決定するには十分ではない部分のみを用いるようにしてもよい。

【 0 0 2 4 】

好ましくは、前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段若しくは初段から段数増加方向へ所定段数隔てた段までの連続する範囲、及び又は最終段若しくは最終段から段数減少方向へ所定段数隔てた段までの連続する範囲に属するラウンド関数に対応する中間状態は、前記拡大鍵として又はそのもととなるデータとして用いないようにしてもよい。また、好ましくは、前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段からの段数と最終段からの段数とが一致する 2 つのラウンド関数に対応する中間状態のいずれか一方又は両方は、前記拡大鍵として又はそのもととなるデータとして用いないようにしてもよい。また、好ましくは、前記ラウンド関数系列に属するラウンド関数のうち、少なくとも、その初段若しくは初段から段数増加方向へ所定段数隔てた段までの連続する範囲、及び又は最終段若しくは最終段から段数減少方向へ所定段数隔てた段までの連続する範囲に属するラウンド関数に対応する中間状態のうち、初段からの段数と最終段からの段数とが一致する 2 つのラウンド関数のいずれか一方又は両方に対応する中間状態は、前記拡大鍵として又はそのもととなるデータとして用いないようにしてもよい。

【 0 0 2 5 】

好ましくは、複数の前記拡大鍵のうちの任意のものが常には一致しないようにしてもよい。また、好ましくは、複数の前記拡大鍵のうちの任意のものが、それら拡大鍵の全ビットのうちの任意のビット群についても、常には一致しないようにしてもよい。

【 0 0 2 6 】

好ましくは、前記ラウンド処理手段及び前記出力手段は、前記データ攪拌処理に必要な拡大鍵数を越える数の拡大鍵を、該データ攪拌処理に提供可能であり、前記提供可能な拡大鍵のうち実際に前記データ攪拌処理に提供すべき拡大鍵を示す情報、又は前記データ攪拌処理に提供すべき拡大鍵及びその提供する順番を示す情報を拡張共通鍵とし、前記出力手段は、前記拡張共通鍵に従って、前記拡大鍵を出力するようにしてもよい。

【 0 0 2 7 】

また、本発明は、暗号化時のデータ攪拌処理と復号時のデータ攪拌処理とで逆の順番で複数の拡大鍵を使用する共通鍵暗号方式による暗号化装置又は復号装置に用いられる拡大鍵生成装置であって、複数段のラウンド関数について、初段では、共通鍵を入力として所定のラウンド関数を施して中間状態を生成し、2段目以降では、前段にて生成された中間状態を入力として所定のラウンド関数を施して新たな中間状態を生成するラウンド処理手段と、前記ラウンド処理手段の全部又は一部の段にて生成された前記中間状態の各々について、該中間状態の全ビット又はその一部をそのまま又はこれに所定の変換処理を施した後に前記拡大鍵として出力するための出力手段とを備え、前記ラウンド処理手段は、複数のラウンド関数を従属接続したラウンド関数系列であって前記共通鍵をその初段へ入力した場合にその最終段が該共通鍵と同一の値を生成するように設定されたラウンド関数系列における全段又はそのうちの一部で初段から連続した複数段についてのラウンド関数を、該ラウンド関数系列の段の順番に従って施すものであることを特徴とする。

【 0 0 2 8 】

なお、暗号化装置に係る本発明は、暗号化方法、復号装置、復号方法、拡大鍵生成装置又は拡大鍵生成方法に係る発明としても成立する。また、それら発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【 0 0 2 9 】

本発明によれば、拡大鍵生成のためのラウンド関数の系列を、共通鍵を入力し、共通鍵と同じ値を出力するように設定することによって、暗号化時と復号時の両方において、従来のような不必要な遅延時間や記憶容量の消費なく、共通鍵から *On-the-fly* に拡大鍵を生成することが可能になる。

【0030】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【0031】

本発明は、暗号化時と復号時とで逆の順番に拡大鍵を用いる共通鍵暗号方式のすべてに適用可能であるが、以下では、所定ビット長のブロック・データに対して逐次的に各拡大鍵を用いたデータ攪拌処理を行っていくような共通鍵ブロック暗号方式を例にとって説明する。

【0032】

まず、本実施形態の基本的な構成例について説明する。

【0033】

なお、以下で参照する各図では（当該暗号に着目して説明するため）暗号対象となるデータを平文として示してあるが、もちろん、暗号対象となるデータがすでに同一のまたは他の暗号方式によって暗号化されたものであってもよい。

【0034】

また、本暗号方式は、ハードウェアによってもソフトウェアによっても実現可能であり、以下に示す構成例は、暗号化装置（復号装置）の機能ブロック図としても成立し、また暗号アルゴリズム（復号アルゴリズム）の機能モジュール図もしくはフローチャート図としても成立する。

【0035】

図1に、本発明の一実施形態に係る暗号化装置の構成例を示す。

【0036】

図1に示されるように、本暗号化装置は、データ攪拌部1と、拡大鍵生成部3を備えている。

【0037】

拡大鍵生成部 3 は、複数のラウンド処理部 3 1 を備えている。

【0038】

f 1 で示したラウンド処理部は、共通鍵 k_c にラウンド関数 f_1 を作用させて中間状態 $k_{c_1} = f_1(k_c)$ を出力する。

f 2 で示したラウンド処理部は、前段のラウンド処理部の出力した中間状態 k_{c_1} にラウンド関数 f_2 を作用させて中間状態 $k_{c_2} = f_2(k_{c_1}) = f_2(f_1(k_c))$ を出力する。

図示しない $f_3 \sim f_{n-1}$ に対応するラウンド処理部も同様である。

f_n で示したラウンド処理部は、前段のラウンド処理部の出力した中間状態 $k_{c_{n-1}}$ にラウンド関数 f_n を作用させて中間状態 $k_{c_n} = f_n(k_{c_{n-1}}) = f_n(f_{n-1}(\dots f_2(f_1(k_c)) \dots))$ を出力する。

【0039】

ここで、本実施形態では、 f_{n+1} で示したラウンド処理部にて前段のラウンド処理部の出力した中間状態 k_{c_n} にラウンド関数 f_{n+1} を作用させ、これによって得られた出力値 $k_{c_n} = f_{n+1}(k_{c_{n-1}}) = f_{n+1}(f_n(f_{n-1}(\dots f_2(f_1(k_c)) \dots)))$ が、共通鍵 k_c に等しくなるようする。また、このラウンド関数 f_{n+1} の逆関数 f_{n+1}^{-1} が、復号装置における拡大鍵生成部の初段のラウンド処理部のラウンド関数になる。なお、図 1 の構成例では、この暗号化装置における拡大鍵生成部にはラウンド関数 f_{n+1} のラウンド処理部を備えなくても構わない（備えても構わない）。

【0040】

また、拡大鍵生成部 3 は、複数の拡大鍵変換部 3 3 を備えている。

【0041】

c_1 で示した拡大鍵変換部は、 f_1 で示したラウンド処理部の出力 k_{c_1} の全部または一部に拡大鍵変換関数 c_1 を作用させて、共通鍵 k_1 を生成する。

c_2 で示した拡大鍵変換部は、 f_2 で示したラウンド処理部の出力 k_{c_2} の全部または一部に拡大鍵変換関数 c_2 を作用させて、共通鍵 k_2 を生成する。

図示しない $c_3 \sim c_{n-1}$ に対応するラウンド処理部も同様である。

c_n で示した拡大鍵変換部は、 f_n で示したラウンド処理部の出力 k_{c_n} の全

部または一部に拡大鍵変換関数 c_n を作用させて、共通鍵 k_n を生成する。

【0042】

データ攪拌部 1 は、ここでは、従属接続された複数の（例えばラウンド関数による）攪拌処理部 11 を備えるものとしている。

【0043】

R_1 で示した攪拌処理部は、暗号化の対象となるブロック・データを入力し、拡大鍵 k_1 を用いて、攪拌処理 R_1 を行う。

R_2 で示した攪拌処理部は、 R_2 で示した攪拌処理部から出力されたブロック・データを入力し、拡大鍵 k_2 を用いて、攪拌処理 R_2 を行う。

図示しない $R_3 \sim R_{n-1}$ に対応する攪拌処理部も同様である。

R_n で示した攪拌処理部は、 R_{n-1} で示した攪拌処理部から出力されたブロック・データを入力し、拡大鍵 k_n を用いて、攪拌処理 R_n を行う。 R_n で示した攪拌処理部の出力が、求めるべき暗号文となる。

【0044】

なお、複数のラウンド関数は、すべて異なるものであっても、すべて同じものであっても、異なるものと同じものが混在するものであってもよい。複数のラウンド関数を異なるものにする場合に、関数を異ならせる方法の他に、基本的には同じ関数であるが段に応じて異なる定数に依存するものにする方法などがある。

また、複数のラウンド関数は、すべて線形関数であっても任意の関数であってもよいが、それらのうちの少なくとも一つを非線形関数にするのが好ましい。また、2以上のラウンド関数あるいは全てのラウンド関数を非線形関数にしてもよい。

また、ラウンド関数は、変換テーブルを用いて実現する方法、行列演算やその他の演算で実現する方法、実回路によって実現する方法など、種々の構成方法がある。

これらの点は、複数の拡大鍵変換関数についても同様である。

なお、拡大鍵生成部 3 として、入力された中間状態またはその一部を、そのまま拡大鍵として出力する構成にする（あるいは、中間状態をデータ攪拌部 1（ま

たは後述するスイッチング回路15)に直結する)ことも可能である。

【0045】

なお、ブロック・データのデータ長と、共通鍵 k_c のデータ長とは、同じであってもよいし、異なるものであってもよい。また、拡大鍵のデータ長と、ブロック・データのデータ長とは、同じであってもよいし、異なるものであってもよい。また、中間状態のデータ長と、拡大鍵のデータ長とは、同じであってもよいし、異なるものであってもよい。

【0046】

図2に、本発明の一実施形態に係る復号装置の構成例を示す。

【0047】

図2に示されるように、本復号装置は、データ攪拌部2と、拡大鍵生成部4を備えている。図2の復号装置は、図1の暗号化装置の逆変換を行う機能を有するものである。

【0048】

拡大鍵生成部4は、複数のラウンド処理部42を備えており、図1の暗号化装置の拡大鍵生成部2の複数のラウンド関数の各々の逆関数を、逆の順番で作用させるものである。

【0049】

f_{n+1}^{-1} で示したラウンド処理部は、共通鍵 $k_c = f_{n+1}(k_{c_n}) = f_{n+1}(f_n(f_{n-1}(\dots f_2(f_1(k_c)) \dots)))$ にラウンド関数 f_{n+1}^{-1} を作用させて、中間状態 $k_{c_n} = f_{n+1}^{-1}(k_c) = f_{n+1}^{-1}(f_{n+1}(f_n(f_{n-1}(\dots f_2(f_1(k_c)) \dots)))) = f_n(f_{n-1}(\dots f_2(f_1(k_c)) \dots))$ を出力する。

f_n^{-1} で示したラウンド処理部は、前段のラウンド処理部の出力した中間状態 k_{c_n} にラウンド関数 f_{n+1}^{-1} を作用させて、 $k_{c_{n-1}} = f_n^{-1}(\dots f_2(f_1(k_c)) \dots)$ を出力する。

図示しない $f_{n-1} \sim f_3$ に対応するラウンド処理部も同様である。

f_2^{-1} で示したラウンド処理部は、前段のラウンド処理部の出力した中間状態 $k_{c_2} = f_2(f_1(k_c))$ にラウンド関数 f_2^{-1} を作用させて、 $k_{c_1} = f$

1 (k c) を出力する。

【 0 0 5 0 】

ここで、本実施形態では、f 1 で示したラウンド処理部にて前段のラウンド処理部の出力した中間状態 k c 2 にラウンド関数 $f 1^{-1}$ を作用させ、これによって得られた出力値は共通鍵 k c に等しくなる。また、このラウンド関数 $f 1^{-1}$ の逆関数 f 1 が、暗号化装置における拡大鍵生成部の初段のラウンド処理部のラウンド関数になる。なお、図 2 の構成例では、この復号装置には拡大鍵生成部ではラウンド関数 $f 1^{-1}$ のラウンド処理部を備えなくても構わない（備えても構わない）。

【 0 0 5 1 】

また、拡大鍵生成部 3 は、複数の拡大鍵変換部 4 4 を備えている。この部分は、図 1 の暗号化装置の対応する部分と同じ処理内容となる。

【 0 0 5 2 】

データ攪拌部 2 は、ここでは、従属接続された複数の（例えばラウンド関数による）攪拌処理部 2 2 を備えるものとしている。

$R n^{-1}$ で示した攪拌処理部は、復号の対象となるブロック・データを入力し、拡大鍵 k n を用いて、暗号化装置の攪拌処理 $R n$ の逆変換となる攪拌処理 $R n^{-1}$ を行う。

同様に、他の攪拌処理部も順次、前段の攪拌処理部から出力されるブロック・データを入力し、拡大鍵 $K n-1$ 、…、または k 2 を用いて、攪拌処理 $R n-1^{-1}$ 、…、または $R 2^{-1}$ を行う。

$R 1^{-1}$ で示した攪拌処理部は、 $R 2^{-1}$ で示した攪拌処理部から出力されたブロック・データを入力し、拡大鍵 k 1 を用いて、暗号化装置の攪拌処理 $R 1$ の逆変換となる攪拌処理 $R 1^{-1}$ を行う。 $R 1^{-1}$ で示した攪拌処理部の出力によって、求めるべき復号結果となるブロック・データが与えられる。

【 0 0 5 3 】

すなわち、復号時において、すぐに暗号化時とは逆の順番での拡大鍵の生成に入り、拡大鍵を次々と生成していくことができる。

【 0 0 5 4 】

以上のように、暗号化時のラウンド関数の系列（ただし、最終段は備えないこともある）と、その逆関数となる復号時のラウンド関数の系列（ただし、最終段は備えないこともある）とについて、暗号化時の最終段の出力に相当する値がもとの共通鍵に一致するようにラウンド関数の系列を設定することによって、暗号化時と復号時の両方において、従来のような不必要な遅延時間や記憶容量の消費なく、共通鍵から $O(n - t h e - f l y)$ に拡大鍵を生成することが可能になる。

【0055】

次に、図1／図2の暗号化装置や復号装置の拡大鍵生成部の複数のラウンド処理部によるラウンド関数の系列について説明する。なお、暗号化装置におけるラウンド関数の系列と、復号装置におけるラウンド関数の系列とは、逆関数の関係になるので、一方が決まれば、他方も決まることになる。ここでは、暗号化装置の方を例にとって説明する。

【0056】

ラウンド関数の系列 f_1, f_2, \dots, f_{n+1} について、そのラウンド関数の系列の内容、あるいは各々の順番のラウンド関数の内容は、当該ラウンド関数の系列が全体として共通鍵を入力し共通鍵と同じ値を出力する条件を満たす範囲内において適宜設定可能であり、様々なバリエーションがある。以下、ラウンド関数の系列のバリエーションのいくつかを例示列挙的に説明する。

【0057】

（ラウンド・トリップ構成）

まず、ラウンド・トリップ構成について説明する。

【0058】

ここでは、ラウンド関数の系列の段数を $2r$ 段とする（なお、前述したように、 $2r$ 段目のラウンド関数は、備えられないことがある）。

【0059】

ラウンド関数の系列を構成する一つの方法は、 $0 \leq i \leq r$ を満たすすべての i について、第 $(r + i)$ 段目の段関数を、第 $(r - i + 1)$ 段目の段関数の逆関数になっている、という関係を満たすように構成する方法である。

【0060】

例えば、ラウンド関数の系列を8段、すなわち、

f_1 、 f_2 、 f_3 、 f_4 、 f_5 、 f_6 、 f_7 、 f_8

とし、 $f_1 \sim f_4$ を任意のラウンド関数として、 $f_5 = f_4^{-1}$ 、 $f_6 = f_3^{-1}$ 、 $f_7 = f_2^{-1}$ 、 $f_8 = f_1^{-1}$ とすると、

f_1 、 f_2 、 f_3 、 f_4 、 f_4^{-1} 、 f_3^{-1} 、 f_2^{-1} 、 f_1^{-1}

という順番の系列となる。すなわち、共通鍵を入力として、 f_1 、 f_2 、 f_3 、 f_4 、 f_4^{-1} 、 f_3^{-1} 、 f_2^{-1} 、 f_1^{-1} を次々と作用させることによって、最終段の出力が共通鍵と一致するようになる。

【0061】

このような構成を、ラウンド・トリップ構成と呼ぶものとする。また、この様子を図3に概念的に示す。

【0062】

ラウンド・トリップ構成を採用した場合、暗号化装置におけるラウンド関数の系列と、復号装置におけるラウンド関数の系列とが同一になる。

【0063】

上記の例の場合、暗号化装置における8段のラウンド関数を、

f_1 、 f_2 、 f_3 、 f_4 、 f_4^{-1} 、 f_3^{-1} 、 f_2^{-1} 、 f_1^{-1}

とすると、復号装置における8段のラウンド関数は、この逆関数となるので、

$(f_1^{-1})^{-1}$ 、 $(f_2^{-1})^{-1}$ 、 $(f_3^{-1})^{-1}$ 、 $(f_4^{-1})^{-1}$ 、 $(f_4)^{-1}$ 、 $(f_3)^{-1}$ 、 $(f_2)^{-1}$ 、 $(f_1)^{-1}$

であり、したがって、

f_1 、 f_2 、 f_3 、 f_4 、 f_4^{-1} 、 f_3^{-1} 、 f_2^{-1} 、 f_1^{-1}

となり、両者が一致することがわかる。

【0064】

なお、暗号化装置においても最終段のラウンド関数（上記の例では、 f_1^{-1} ）を備えなくてもよいし、復号装置においても最終段のラウンド関数（上記の例では、 f_1 ）を備えなくてもよいが、いずれも最終段のラウンド関数を備えれば、構成が同一となるので、暗号化機能と復号機能の両方の機能を兼ね備えさせる装置においては、暗号化時と復号時とで1つの拡大鍵生成部を兼用することによ

て、装置規模を削減することも可能である。

【0065】

次に、この構成において、ラウンド関数の系列の前半の各ラウンド関数は、すべて異なるものであっても、すべて同じものであっても、異なるものと同じものが混在するものであってもよい。

【0066】

例えば、ラウンド関数の系列の前半の各ラウンド関数がすべて同じものである場合、段数を8段とすると、暗号側と復号側のいずれにおいても、

$$f_1, f_1, f_1, f_1, f_1^{-1}, f_1^{-1}, f_1^{-1}, f_1^{-1}$$

という系列になる。

【0067】

ところで、ラウンド・トリップ構成を採用した場合、ラウンド関数の系列において逆関数の関係にある対応部分の中間状態が同一になる。したがって、同一の中間状態に同一の拡大鍵変換関数を作用させると、同一の拡大鍵が生成される。そこで、これを避けるために、ラウンド関数の系列において逆関数の関係にある対応部分についての2つの拡大鍵変換部の拡大鍵変換関数として相異なるものを用いるようにしてもよい。

【0068】

例えば、8段のラウンド関数の系列を、

$$f_1, f_2, f_3, f_4, f_4^{-1}, f_3^{-1}, f_2^{-1}, f_1^{-1}$$

とし、 f_1 の出力を用いる拡大鍵変換関数を c_1 、…、 f_2^{-1} の出力を用いる拡大鍵変換関数を c_7 とすると、拡大鍵変換関数 c_1 と拡大鍵変換関数 c_7 とを異ならせるようにしてもよい。 c_2 と c_6 、 c_3 と c_5 についても同様である。

【0069】

(ループ構成)

次に、ループ構成について説明する。

【0070】

ラウンド・トリップ構成では、ラウンド関数の系列の後半を、その前半の逆関数としたが、ラウンド関数の系列の中の部分系列として、ラウンド・トリップ構

成に相当する部分を全く持たない構成も可能である。

【0071】

このような構成を、ループ構成と呼ぶものとする。また、この様子を図4に概念的に示す。

【0072】

なお、ラウンド・トリップ構成では、ラウンド関数の系列の段数を偶数段としたが、ループ構成では、ラウンド関数の系列の段数は、偶数段であっても奇数段であってもよい。

【0073】

例えば、ラウンド関数の系列を8段とした場合に、共通鍵を入力として、
 f_1 、 f_2 、 f_3 、 f_4 、 f_5 、 f_6 、 f_7 、 f_8
 を次々と作用させることによって、最終段の出力が共通鍵と一致するようにする。
 この場合、その逆関数は、

f_{8-1} 、 f_{7-1} 、 f_{6-1} 、 f_{5-1} 、 f_{4-1} 、 f_{3-1} 、 f_{2-1} 、 f_{1-1}
 であり、共通鍵を入力すると、最終段の出力が共通鍵と一致することになる。

【0074】

また、例えば、ラウンド関数の系列の前半の各ラウンド関数がすべて同じものである場合、段数を8段とすると、暗号側では、

f_1 、 f_1 、 f_1 、 f_1 、 f_1 、 f_1 、 f_1 、 f_1
 という系列になり、

復号側では、

f_1^{-1} 、 f_1^{-1} 、 f_1^{-1} 、 f_1^{-1} 、 f_1^{-1} 、 f_1^{-1} 、 f_1^{-1} 、 f_1^{-1}
 という系列になる。

【0075】

なお、このような条件を満たす関数は、シフト演算、行列演算、ガロア体演算など、種々のものがある。

【0076】

(ラウンド・トリップ／ループ複合構成)

ラウンド関数の系列としては、その部分系列として、ラウンド・トリップ構成

に相当する部分と、ループ構成に相当する部分とを複合的に備えるような構成も可能である。

【0077】

以下、ラウンド・トリップ構成部分を図3の表記方法で示し、ループ構成部分を図3の表記方法で示すものとして、図5～図9にいくつかのバリエーションを例示する。

【0078】

図5の例は、ラウンド・トリップ構成部分の途中にラウンド・トリップ構成部分を含むような入れ子構造になっているものである。図5の場合のラウンド関数の系列を例示すると、

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow b_1 \rightarrow b_2 \rightarrow b_2^{-1} \rightarrow b_1^{-1} \rightarrow a_4 \rightarrow a_5 \rightarrow a_6 \rightarrow a_6^{-1} \rightarrow a_5^{-1} \rightarrow a_4^{-1} \rightarrow a_3^{-1} \rightarrow c_1 \rightarrow c_2 \rightarrow c_2^{-1} \rightarrow d_1 \rightarrow d_1^{-1} \rightarrow c_1^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1}$$

となる。

この例の場合、 $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_4 \rightarrow a_5 \rightarrow a_6 \rightarrow a_6^{-1} \rightarrow a_5^{-1} \rightarrow a_4^{-1} \rightarrow a_3^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1}$ というラウンド・トリップ構成の中に、 $b_1 \rightarrow b_2 \rightarrow b_2^{-1} \rightarrow b_1^{-1}$ というラウンド・トリップ構成と、 $c_1 \rightarrow c_2 \rightarrow c_2^{-1} \rightarrow c_1^{-1}$ というラウンド・トリップ構成が入っており、さらに、 $c_1 \rightarrow c_2 \rightarrow c_2^{-1} \rightarrow c_1^{-1}$ というラウンド・トリップ構成の中に、 $d_1 \rightarrow d_1^{-1}$ というラウンド・トリップ構成が入っている。

【0079】

図6の例は、ループ構成部分の途中にループ構成部分を含むような入れ子構造になっているものである。図6の場合のラウンド関数の系列を例示すると、

$$s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow t_1 \rightarrow t_2 \rightarrow t_3 \rightarrow s_5 \rightarrow s_6 \rightarrow s_7 \rightarrow s_8$$

となる。

この例の場合、 $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow s_5 \rightarrow s_6 \rightarrow s_7 \rightarrow s_8$ というループ構成の中に、 $t_1 \rightarrow t_2 \rightarrow t_3$ というループ構成が入っている。

【0080】

図7の例は、ループ構成部分の途中にラウンド・トリップ構成部分を含むよう

な構造になっているものである。図7の場合のラウンド関数の系列を例示すると

$$s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow s_5 \rightarrow a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_3^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1} \\ \rightarrow s_6 \rightarrow s_7 \rightarrow s_8 \rightarrow s_9$$

となる。

この例の場合、 $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow s_5 \rightarrow s_6 \rightarrow s_7 \rightarrow s_8 \rightarrow s_9$ というループ構成の中に、 $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_3^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1}$ というラウンド・トリップ構成が入っている。

【0081】

図8の例は、ラウンド・トリップ構成部分の途中にループ構成部分を含むような構造になっているものである。図8の場合のラウンド関数の系列を例示すると

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_4 \rightarrow a_5 \rightarrow a_6 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow a_6^{-1} \rightarrow a_5^{-1} \\ \rightarrow a_4^{-1} \rightarrow a_3^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1}$$

となる。

この例の場合、 $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_4 \rightarrow a_5 \rightarrow a_6 \rightarrow a_6^{-1} \rightarrow a_5^{-1} \rightarrow a_4^{-1} \rightarrow a_3^{-1} \rightarrow a_2^{-1} \rightarrow a_1^{-1}$ というラウンド・トリップ構成の中に、 $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4$ というループ構成が入っている。

【0082】

図9の例は、4つのラウンド・トリップ構成部分と、2つのループ部分を持つものである。

【0083】

もちろん、これら以外にも、ラウンド・トリップ構成部分とループ構成部分の組み合わせ方、あるいは階層構造の取り方など、種々のバリエーションが可能である。

【0084】

さて、図1／図2の構成例は、データ攪拌部で必要とする数の分だけ拡大鍵を生成することを想定したものであったが、データ攪拌部で必要とする数を越える数の分の拡大鍵を生成可能とするラウンド関数の段数を備え、生成可能な拡大鍵

の一部をデータ攪拌部で使用する構成も可能である。

【0085】

この場合の図1／図2の暗号化装置／復号装置に対応する構成例を、図10／図11にそれぞれ示す。

【0086】

ここでは、図1／図2と相違する点を中心に説明する。もちろん、ラウンド関数の系列は、上記したラウンド・トリップ構成等を採用したものであってよい。

【0087】

図10の5と図11の6は、拡大鍵 k_i と攪拌処理 R_j との接続関係を示す部分であり、そのいくつかの具体例を図12～図15に例示している。なお、本実施形態では、図10の5の接続関係と図11の6の接続関係は同一になる。

【0088】

なお、ここでは、初段のラウンド関数への入力としての共通鍵と、最終段のラウンド関数からの出力されることになる共通鍵の双方または一方をも、中間状態として拡大鍵生成に利用してもよい。なお、後者を用いる場合に、実際に最終段のラウンド関数の出力を用いるようにしてもよいし、共通鍵を記憶しておいてこれを用いるようにしてもよい。

【0089】

本実施形態では、生成可能な拡大鍵の数が、攪拌処理に必要な拡大鍵の数より多くなるように構成し、拡大鍵 k_i と攪拌処理 R_j とを適宜対応付ける。なお、同一の拡大鍵を複数の攪拌処理に使用可能とする方法と、1つの拡大鍵を攪拌処理について排他的に使用可能とする方法とがある。

【0090】

なお、使用しないことになる拡大鍵は、生成しないようにして構わない。この場合には、対応する拡大鍵変換部を備えなくて構わない。

【0091】

このように生成しうる拡大鍵の一部のみをデータ攪拌に使用する構成は、攻撃に対する安全性の面で効果的である。

【0092】

以下、種々のバリエーションについて説明する。

【0093】

まず、データ攪拌部の攪拌処理の段数が n であり、（拡大鍵変換部を備えたとして）生成可能な拡大鍵の個数が m （ $m > n$ ）である場合に、基本的には、拡大鍵の重複使用を許さない構成では、 m 個の拡大鍵のうちから n 個の拡大鍵を任意に選択したすべての組み合わせが可能である。なお、ここでは、生成される順番に拡大鍵を使用するものとする。

【0094】

なお、拡大鍵の重複使用を許す構成では、基本的には、 n^m 通りの組み合わせが可能である。

【0095】

いずれの拡大鍵を選択するかについては、ランダムに選択する方法の他に、所定の基準に従って選択する方法がある。

【0096】

SQUARE 攻撃と呼ばれる特殊な攻撃では、従来の暗号方式に対して、初段（あるいは最初からの連続する数段）あるいは最終段（あるいは最終段までの連続する数段）の拡大鍵のうち一部のビットに対して、全数探索が行われる。この場合、初段と最終段の拡大鍵が同一である場合には、探索の空間が小さくなってしまい、解読される可能性が高くなる。

【0097】

そこで、初段の拡大鍵変換部により得られる拡大鍵（以下、初段の拡大鍵と呼ぶ）と最終段の拡大鍵変換部により得られる拡大鍵（以下、最終段の拡大鍵と呼ぶ）については、高々一方のみをデータ攪拌に使用するようにしてもよい（いずれか一方のみをデータ攪拌に使用する方法と、いずれもデータ攪拌に使用しない方法とがある）。

【0098】

また、同様に、初段からの連続する数段分の拡大鍵と最終段までの連続する数段分の拡大鍵の範囲において、初段または最終段からの段数を同じくする2つの段の拡大鍵の組について、いずれの組においても、高々一方のみをデータ攪拌に

使用するようにしてもよい。この場合に、使用するものあるいは使用しないものについての選択方法には種々のバリエーションが考えられる。例えば、いずれの組においても、いずれか一方を使用するものとする場合に、各組ごとに、使用する方（または使用しない方）を、ランダムに選択してもよいし、例えば前半と後半とから交互になるように選択するなど一定の基準に従って選択するようにしてもよい。また、例えば、各組ごとに、段の順番が前側のものを使用するか、段の順番が後ろ側のものを使用するか、いずれも使用しないかを、ランダムに選択してもよいし、一定の基準に従って選択するようにしてもよい。

例えば、図12に示すように、拡大鍵が15段分生成可能であり、攪拌処理が9段ある場合に、初段の拡大鍵k1と最終段の拡大鍵k15のうちではk15を使用し、その1つ内側の段のk2とk14のうちからはk2を使用し、同様に、k3とk13のうちからはk13を使用し、k4とk12のうちからはk4を使用し、k5とk11のうちからはk11を使用し、k6とk10のうちからはk6を使用するようにしてもよい。なお、この場合においても、生成される順番に拡大鍵を使用するようにしている。

【0099】

また、初段からの連続する数段分の拡大鍵と最終段までの連続する数段分の拡大鍵の範囲については使用しないようにしてもよい。図13に、このときの様子を示す。

【0100】

また、初段と最終段、または初段からの連続する数段分の拡大鍵と最終段までの連続する数段分の拡大鍵の範囲については使用せず、その内側の連続する数段分の拡大鍵の範囲については前述と同様に対応する1組のうち的一方のみを使用するようにしてもよい。図14に、このときの様子を示す。

【0101】

もちろん、以上の例の他にも、種々のバリエーションがある。

【0102】

ところで、これまでは、拡大鍵を生成可能な順番で、データ攪拌に使用するものとして説明したが、メモリ等のハードウェアまたは計算時間にある程度の余裕

があれば、その余裕に応じて、拡大鍵が生成される順番と、拡大鍵をデータ攪拌に使用する順番とを入れ替えるようにしてもよい。この順番の入れ替えは、図 1 や図 2 の構成においても同様である。この順番の入れ替えも、攻撃に対する安全性の面で効果的である。

【 0 1 0 3 】

図 1 5 に、拡大鍵が生成される順番と、拡大鍵をデータ攪拌に使用する順番とを入れ替えた例を示す。

【 0 1 0 4 】

なお、順番を入れ替える場合には、例えば、先に生成された拡大鍵を、後に生成された拡大鍵よりも後で使用するために、一旦、メモリに格納しておくようにすればよい。1 つの拡大鍵の順番を入れ替えるだけならば、1 つの拡大鍵を一時保存するのに必要なメモリ容量が増加するだけである。

【 0 1 0 5 】

メモリを増加させないためには、中間状態にラウンド関数の逆関数を作用させて必要な中間状態を復元させればよい。例えば、初段のラウンド関数 f_1 による中間状態 k_{c_1} から得られる拡大鍵 k_1 を、2 段目のラウンド関数 f_2 による中間状態 k_{c_2} から得られる拡大鍵 k_2 を使用した後に使用する場合、一旦、中間状態 k_{c_2} を求めた後に、 k_{c_2} に 2 段目のラウンド関数 f_2 の逆関数 f_2^{-1} を作用させて中間状態 k_{c_1} を求め（これによって拡大鍵 k_1 が得られる）、さらに中間状態 k_{c_1} に 2 段目のラウンド関数 f_2 を作用させて中間状態 k_{c_2} を求め、これに 3 段目のラウンド関数 f_3 を作用させる…、というようにすることによって、使用順に拡大鍵を生成することができる。なお、ラウンド関数系列がラウンド・トリップ構成を有する場合には、ラウンド関数 f_2 の逆関数 f_2^{-1} も同時に備えているので、これを上記の処理に利用するようにしてもよい。

【 0 1 0 6 】

ところで、以上の拡大鍵の選択や順序の入れ替えは、固定的なものであったが、これを可変とするようにしてもよい。

【 0 1 0 7 】

この場合の図 1 0 / 図 1 1 の暗号化装置 / 復号装置に対応する構成例を、図 1

6 / 図 1 7 にそれぞれ示す。図中の 7 と 8 はデコーダであり、1 5 と 1 6 はスイッチング回路である。

【0 1 0 8】

この場合、予め各々の攪拌処理 R_j へ拡大鍵 k_i を対応付ける接続パターン（図 1 2 等参照）を複数種類用意しておき、各パターンをコード化し、これを拡張共通鍵 $k_{c'}$ として、本来の共通鍵 k_c に付加する。

【0 1 0 9】

暗号化時には、拡張共通鍵 $k_{c'}$ は、デコーダ 7 に与えられ、デコーダ 7 は、拡張共通鍵 $k_{c'}$ を解読し、該拡張共通鍵 $k_{c'}$ が示す接続パターン（例えば、図 1 2 等のパターン）を実現するようにスイッチング回路 1 5 に対するスイッチング制御を行う。

これらの動作は、復号時も同様である。

【0 1 1 0】

なお、上記では、パターンをコード化するようにしたが、その代わりに、使用しない拡大鍵の段数を示す情報など、他の形態の情報を用いることも可能である。

【0 1 1 1】

このような構成も、攻撃に対する安全性の面で効果的である。

【0 1 1 2】

なお、以上の各構成例において、図 1 8 に示すように、初段および最終段に擬アダマール変換のような補助関数を挿入するようにしてもよい。この場合に、初段の補助関数と最終段の補助関数に同一の拡大鍵（例えば、初段の拡大鍵）を用いるようにしてもよい。なお、擬アダマール変換は、例えば、ブロック・データの左半分と右半分の算術加算を取ったものを新たな左半分とし、この新たな左半分と右半分の算術加算を取ったものを新たな右半分とするような処理が、これに該当する。

【0 1 1 3】

以下では、暗号化装置や復号装置の拡大鍵生成部の複数の拡大鍵変換部のバリエーションについて説明する。

【0114】

図19には、1つの拡大鍵生成部の構成例を示す。図19において、101は8ビットのS-boxであり、103はMDS (Maximum Distance Separable; 最大距離分離) 行列に基づく32ビットの攪拌部である。この例は、中間状態の全部または一部として $32 \times k$ ビットのデータを入力し、 $32 \times k$ ビットの拡大鍵を出力するもので、4並列のS-box 101に攪拌部 103を接続したものを1単位として、これをk個分並列に設けたものである。

【0115】

もちろん、前述したように、拡大鍵生成部は、種々の構成が可能である。

【0116】

ところで、ある種の暗号解読によりある段（一般には最終段）の拡大鍵（の一部）が知られるおそれは完全には否定できない。かりに、ある段の拡大鍵が知られてしまった場合、拡大鍵変換部の逆変換を行うことで、その段の（ラウンド関数についての）中間状態を知られてしまい、その結果として、他の段の中間状態すべてが知られるところとなり、結局、すべての拡大鍵が知られるところとなるおそれがある。

そこで、一部（例えば最終段を含む1段または数段）の拡大鍵変換部においては、逆変換が容易でない関数（例えば、べき乗関数）や、逆が一意に定まらない関数（例えば、多対一関数）を用いるようにしてもよい。これによって、他の段の拡大鍵を容易には知られないようにすることが可能になり、安全性を維持することができる。もちろん、全部の拡大鍵変換部について、逆変換が容易でない関数や、逆が一意に定まらない関数を用いるようにしてもよい。

【0117】

また、拡大鍵変換部には、対応する段の中間状態の全データを与えてもよいが、その代わりに、対応する段の中間状態の一部のみを渡す構成にして、中間状態の全データを知られないようにし、これによって安全性を維持することもできる。

【0118】

また、サイドチャネル解析と呼ばれる特殊な攻撃では、ハードウェアで構成された暗号化装置に対して、電力、電磁波等、ＩＣカード等の装置から漏洩する情報をもとに鍵の推測を行う。特に、データ攪拌処理におけるある回路において、同一の構成を有する複数の回路部分があり、それらの回路への入力ビット列とその回路で使用される鍵ビット列（拡大鍵自体または拡大鍵の一部のデータ）が同一であったならば、サイドチャネル情報（例えば、消費電流の変化）の同一性から、それら回路について、入力されたビット列が同一であったことが推測されてしまう。したがって、拡大鍵生成においては、ＩＣカード等で問題となるサイドチャネル解析が容易となるような鍵を生成しないものが望まれる。

【 0 1 1 9 】

そこで、少なくとも処理要素（回路部分）の入出力の一部が直接観測あるいは推定が可能な相異なる処理要素（回路部分）において、同一の拡大鍵が使われないような拡大鍵生成方法が有効である。

【 0 1 2 0 】

なお、全拡大鍵が常には一致しないように、拡大鍵変換部、または拡大鍵変換部およびラウンド処理部、またはラウンド処理部を設計し、偶然一致することは許すようにしてもよい。

【 0 1 2 1 】

また、全拡大鍵が常には一致しないように、拡大鍵変換部、または拡大鍵変換部およびラウンド処理部、またはラウンド処理部を設計するとともに、共通鍵の生成時に、全拡大鍵が異なるかどうかをチェックし、全拡大鍵が異なると判定された場合にのみ、その共通鍵を使用するようにしてもよい。

【 0 1 2 2 】

ここで、拡大鍵の一致については、様々なレベルが考えられる。例えば、２つの拡大鍵の全ビットが同一のときに、一致したと判断するようにしてもよい。また、２つの拡大鍵の特定のバイト位置のデータが同一のときには、一致したと判断するようにしてもよい。また、２つの拡大鍵の全ビット、または２つの拡大鍵の特定のバイト位置のデータの間に、一定の関係があるときには、一致したと判断するようにしてもよい。これらの他にも、種々の一致判定方法が可能である。

【 0 1 2 3 】

以下では、暗号化装置や復号装置の拡大鍵生成部の複数のラウンド処理部のバリエーションについて説明する。

【 0 1 2 4 】

図 2 0 には、ラウンド処理部の系列の構成例を示す。図 2 0 の例では、3 段分示してあるが、各段の構成が所定段数従属接続されることになる。また、図 2 0 では、共通鍵が 1 2 8 ビットであり、各段の拡大鍵は 6 4 ビットである場合を例示している。図中、1 0 5 は非線形写像 F であり、1 0 7 の記号は排他的論理和を示している。

【 0 1 2 5 】

非線形写像 F は、全段で同一であってもよいし、段ごとに異なってもよい。また、後者の場合、基本的には、同じ構成を有するが、段に応じて異なる定数に依存するものであってもよい。

【 0 1 2 6 】

なお、図 2 0 と図 2 0 の逆関数のいずれを暗号化側（または復号側）に用いることも可能である。

【 0 1 2 7 】

一般に、差分解読法や線形解読法といった強力な解読法を用いても、最終段の拡大鍵のうち高々数ビットを特定するのが限界であるから、ラウンド関数の系列は、図 2 0 に示したような単純な Feistel 構造でも安全性に大きな問題は無いと考えられるが、もし、より強力な解読法の出現に備えてより安全な構造を望むならば、例えば図 2 1 に示すようなラウンド関数の系列を用いてもよい。

【 0 1 2 8 】

図 2 1 の例では、2 段分示してあるが、各段の構成が所定段数従属接続されることになる。また、図 2 1 では、共通鍵が 1 2 8 ビットであり、各段の拡大鍵は 6 4 ビットである場合を例示している。図中、1 0 9 と 1 1 1 と 1 1 3 はそれぞれ非線形関数 f と g と h を示しており、1 1 5 の記号は排他的論理和を示している。非線形関数 f と g と h は、すべて同一であっても、すべて異なっても、それらのうち一部のもの同士のみ同一でもよい。

【 0 1 2 9 】

図 2 2 に、非線形関数 f や g や h の構成例を示す。図 2 2 において、1 1 9 は 8 ビットの $S - b o x$ であり、1 2 1 は M D S 行列に基づく 3 2 ビットの攪拌部である。

【 0 1 3 0 】

図 2 1 では、図 2 0 に比較して、出力される 1 2 8 ビットから中間状態を一意に決定することがより困難になっている。

【 0 1 3 1 】

図 2 3 に、図 2 1 の逆関数を示す。なお、図 2 1 と図 2 3 のいずれを暗号化側（または復号側）に用いることも可能である。

【 0 1 3 2 】

以下では、本発明を適用した暗号化装置の一具体例を示す。

【 0 1 3 3 】

図 2 4 に、本暗号化装置の構成例を示す。

【 0 1 3 4 】

この暗号化装置は、1 2 8 ビット（6 4 ビット）のブロック暗号であり、共通鍵は 2 5 6 ビット（1 2 8 ビット）であり、1 段の 2 5 6 ビット（1 2 8 ビット）である場合を例にとっている。また、ラウンド関数の系列は、ラウンド・トリップ構成を有する場合を例にとっている。また、通常の S P N 構造の $S - b o x$ の部分に小型の S P N 構造を再帰的に埋め込んだ入れ子型 S P N 構造である場合を例にとっている。

【 0 1 3 5 】

図 2 4 において、データ攪拌部では、ラウンド関数（D U）2 0 1 とラウンド関数（D D）2 0 3 の繰り返し構造の後、ラウンド関数（D U）2 0 1 とラウンド関数（D D（w o M D S H））2 0 5 と、ラウンド関数（E X O R）2 0 7 が接続されている。

【 0 1 3 6 】

また、拡大鍵生成部では、ユニット 2 0 9 とユニット 2 1 1 の対が 1 段分のラウンド関数に相当する。ただし、図 2 4 の例では、ユニット 2 0 9 とユニット 2

09の間およびユニット211とユニット211の間が図1の中間状態ではなく、中間状態はユニット209やユニット211の内部に現れる構造になっている。

【0137】

図25に、128ビットのブロック暗号の場合における、図24のユニット201の構成例を示す。図25において、215は鍵加算のための8ビットの排他的論理和であり、217は8ビットのS-boxであり、219はMDS行列に基づく32ビットの攪拌部である。213のユニットが4並列に設けられる。

なお、64ビットのブロック暗号の場合には、213のユニットが2並列に設けられる。

【0138】

図26に、128ビットのブロック暗号の場合における、図24のユニット202の構成例を示す。図26において、221は鍵加算のための8ビットの排他的論理和であり、223は16並列の8ビットのS-boxであり、225はMDS行列に基づく128ビットの攪拌部である。

なお、64ビットのブロック暗号の場合には、223のS-boxが8並列に設けられる。

【0139】

図27に、128ビットのブロック暗号の場合における、図24のユニット205の構成例を示す。図27において、227は鍵加算のための8ビットの排他的論理和であり、229は16並列の8ビットのS-boxである。

なお、64ビットのブロック暗号の場合には、229のS-boxが8並列に設けられる。

【0140】

ユニット207は、128ビットのブロック暗号の場合、ユニット205から出力される128ビットのブロック・データに128ビットの拡大鍵を加算するための排他的論理和である。

また、ユニット207は、64ビットのブロック暗号の場合、ユニット205から出力される64ビットのブロック・データに64ビットの拡大鍵を加算する

ための排他的論理和である。

【0141】

図28に、共通鍵のビット長が256ビットの場合における図24の拡大鍵生成部の構成例を示す。図28では、初段部分と折り返し部分のみについて示している。図中、231は非線形関数Fであり、233は排他的論理和であり、235は段に依って異なる定数との排他的論理和である。237、239、241、243のユニットについては後述する。

【0142】

図29に、共通鍵のビット長が128ビットの場合における図24の拡大鍵生成部の構成例を示す。図29では、初段部分と折り返し部分のみについて示している。図中、251は非線形関数Fであり、253は排他的論理和であり、255は段に依って異なる定数との排他的論理和である。257、259、261、263のユニットについては後述する。

【0143】

図30に、図28の非線形関数231の構成例を示す。図中、2311は排他的論理和であり、2313はS-boxであり。2315、2317については後述する。

【0144】

次に、図28のP32と示されたユニット237、図29のP16と示されたユニット257、図30のP16と示されたユニット2315、図30のP8と示されたユニット2317について説明する。図31に、これらに共通する一般的な構成例を示す。図中、265は排他的論理和であり、あるiビットと他のiビットとの排他的論理和を取る操作が4回行われる。この構成をPiで表現したものが、各図のP8、P16、P32である。すなわち、図28のユニット237は図31の構成でi=32としたものであり、図29のユニット257は図31の構成でi=16としたものであり、図30のユニット2315は図31の構成でi=16としたものであり、図30のユニット2317は図31の構成でi=8としたものである。

【0145】

図32に、図31の P_i の逆変換である P_i^{-1} の構成例を示す。図中、267は排他的論理和である。図28のユニット243は図31の構成で $i=32$ としたものであり、図29のユニット263は図31の構成で $i=16$ としたものである。

【0146】

なお、図30は、128ビットのブロック暗号の場合であったが、64ビットのブロック暗号の場合、すなわち図29の非線形関数251の場合には、図30において、P8をP4にし、P16をP8にすればよい。

【0147】

次に、図28／図29の5と示されたユニット239／259、図29／図30のBと示されたユニット241／261について説明する。図33に、5と示されたユニットおよびBと示されたユニットの構成例を示す。両者の違いは、図33のユニット269における関数の内容である。

【0148】

図33の構成は、ガロア体 $GF(2^4)$ の元5、またはBを乗じるものである。

【0149】

すなわち、入力となる32ビットを、4組の8ビットに分け、8ビット・データの同じ位置（例えば図33では最上位ビットの最下位ビットを例にとって示している）の1ビットを集めて、これを1組4ビットのデータとし、8組の4ビット・データの各々を、 $GF(2^4)$ の元とみなす。そして、各々の4ビット・データに対し各々のユニット269によって（ガロア体上の乗算に従って）5またはBを乗じた後に、各々のビットをそれぞれ対応するもとの位置に戻す。

【0150】

なお、上記では、同じ位置のビットを取り出して処理を行うものとして説明したが、異なる位置のビットを（排他的に）取り出して処理を行うことも可能である。

【0151】

ガロア体上の乗算は、表引きによっても、演算によっても、実回路によっても

よい。

【0152】

図34に、図33のユニット269の部分の構成例、すなわち $GF(2^4)$ 上の乗算の結線表現（結線パターン）を、元5について（a）に、元Bについて（b）にそれぞれ示す。なお、前述したように、結合部分271では、排他的論理和がなされる。すなわち、この場合、図28／図29の5と示されたユニット239／259については、図33および図34（a）によって構成可能であり、図29／図30のBと示されたユニット241／261については、図33および図34（b）によって構成可能である。

【0153】

ところで、データ攪拌部の拡大鍵を作用させる対象が既知あるいは比較的容易に推測可能な部分で使用される拡大鍵、例えばデータ攪拌部の最初の排他的論理和演算や、出力と鍵の推測からデータの推定が可能となる最後の鍵加算の前の排他的論理和演算部への拡大鍵において、異なる位置の演算要素単位（この例の場合、8ビット単位）で拡大鍵が常に一致することや常に一定の関係を持つことを防ぐようにすると好ましい。

一構成例としては、上記のデータ攪拌部の最初の排他的論理和演算で使用される拡大鍵と、最後の鍵加算の前の排他的論理和演算部への拡大鍵に要素単位（この例の場合、8ビット単位）で常に成り立つ一致が発生しないように、拡大鍵を生成する（もしくは共通鍵を選択する）。これにより、サイドチャネル解析を容易ならしめる拡大鍵の一致や一定の関係の成立を妨げることができる。

【0154】

なお、図24に対応する復号装置の構成は、データ攪拌部については図24のデータ攪拌部の逆関数になる。また、拡大鍵生成部については、暗号側と復号側ともに最終段のラウンド関数を備えた場合には、図24の拡大鍵生成部と同様の構成になる。もちろん、暗号側も復号側もそれぞれ最終段のラウンド関数を備えなくてもよい。

【0155】

なお、図1～図34を参照しながら説明してきた以上のような実施形態におい

て、128ビット等の特定のビット長を例にとったが、もちろん、どのようなビット長のブロックデータでも適用可能である。

また、データ攪拌部は、どのような構成であっても適用可能である。

【0156】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【0157】

本実施形態の暗号化装置や復号装置は、ハードウェアとしても、ソフトウェアとしても、実現可能である。

【0158】

本実施形態は、ソフトウェアで実現する場合に、暗号化装置や復号装置を実現するプログラムであって、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0159】

また、ハードウェアとして構成する場合、半導体装置として形成することができる。

【0160】

また、本発明を適用した暗号化装置や復号装置を構成する場合、あるいは暗号化プログラムや復号プログラムを作成する場合に、ブロックもしくはモジュールをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては1または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【0161】

また、ソフトウェアの場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【0162】

なお、暗号化機能を持ち、復号機能を持たない装置として構成することも、復

号機能を持ち、暗号化機能を持たない装置として構成することも、暗号化機能と復号機能の両方を持つ装置として構成することも、可能である。同様に、暗号化機能を持ち、復号機能を持たないプログラムとして構成することも、復号機能を持ち、暗号化機能を持たないプログラムとして構成することも、暗号化機能と復号機能の両方を持つプログラムとして構成することも、可能である。

【 0 1 6 3 】

次に、本実施形態のシステムへの応用について説明する。

【 0 1 6 4 】

本実施形態の暗号方式は、基本的にはどのようなシステムにも適用可能である。

【 0 1 6 5 】

例えば、図 3 5 に示すように、送信側装置 3 0 1 と、受信側装置 3 0 3 との間で、所定の方法もしくは手続により、鍵を安全に共有しておき、送信側装置 3 0 1 は送信データをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のプロトコルに従って、通信ネットワーク 3 0 2 を介して、暗号文を受信側装置 3 0 3 へ送信し、暗号文を受信した受信側装置 3 0 3 では、受信した暗号文をブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。なお、各々の装置が、暗号化機能と復号機能を両方持っていれば、双方向に暗号通信を行うことができる。

【 0 1 6 6 】

また、例えば、図 3 6 に示すように、計算機 3 1 1 では、所定の方法で鍵を生成し、保存したいデータをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のネットワーク（例えば、LAN、インターネット等）3 1 4 を介して、暗号化データとして、データ・サーバ 3 1 3 に保存しておく。計算機 3 1 1 では、このデータを読みたいときは、データ・サーバ 3 1 3 から所望の暗号化データを読み込み、これをブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。また、他の計算機 3 1 2 が、この鍵を知っていれば、同様に復号してもとの平文を得ることができるが、鍵の分からない他の計算機は、該暗号データを復号することはできず、情報のセキュリティ・コントロールが可能

になる。

【0167】

また、例えば、図37に示すように、コンテンツ提供側では、暗号化装置321により、あるコンテンツを、ある鍵で、ブロック長ごとに本実施形態の暗号方式で暗号化し、これを暗号化コンテンツとして、記録媒体322に記録し、これを頒布等する。記録媒体322を取得したユーザ側では、所定の方法で該ある鍵を入手することにより、復号装置323により、該コンテンツを、ブロック長ごとに本実施形態の暗号方式で復号し、コンテンツの閲覧もしくは再生等を行うことができる。

【0168】

もちろん、上記以外にも種々のシステムに適用可能である。

【0169】

なお、本実施形態で示した各々の構成は、一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、本実施形態は、暗号化装置としての発明、復号化装置としての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【0170】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【 0 1 7 1 】

【発明の効果】

本発明によれば、拡大鍵生成のためのラウンド関数の系列を、共通鍵を入力し、共通鍵と同じ値を出力するように設定することによって、暗号化時と復号時の両方において、従来のような不必要な遅延時間や記憶容量の消費なく、共通鍵から *On-the-fly* に拡大鍵を生成することが可能になる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る暗号化装置の構成例を示す図

【図 2】

同実施形態に係る復号装置の構成例を示す図

【図 3】

ラウンド関数の系列の構成について説明するための図

【図 4】

ラウンド関数の系列の構成について説明するための図

【図 5】

ラウンド関数の系列の構成について説明するための図

【図 6】

ラウンド関数の系列の構成について説明するための図

【図 7】

ラウンド関数の系列の構成について説明するための図

【図 8】

ラウンド関数の系列の構成について説明するための図

【図 9】

ラウンド関数の系列の構成について説明するための図

【図 1 0】

同実施形態に係る暗号化装置の他の構成例を示す図

【図 1 1】

同実施形態に係る復号装置の他の構成例を示す図

【図 1 2】

拡大鍵と攪拌処理との接続関係例を示す図

【図 1 3】

拡大鍵と攪拌処理との接続関係例を示す図

【図 1 4】

拡大鍵と攪拌処理との接続関係例を示す図

【図 1 5】

拡大鍵と攪拌処理との接続関係例を示す図

【図 1 6】

同実施形態に係る暗号化装置のさらに他の構成例を示す図

【図 1 7】

同実施形態に係る復号装置のさらに他の構成例を示す図

【図 1 8】

同実施形態に係る暗号化装置のさらに他の構成例を示す図

【図 1 9】

同実施形態に係る拡大鍵生成部の構成例を示す図

【図 2 0】

同実施形態に係るラウンド処理部の構成例を示す図

【図 2 1】

同実施形態に係るラウンド処理部の他の構成例を示す図

【図 2 2】

図 2 1 のラウンド処理部の非線形関数ユニットの構成例を示す図

【図 2 3】

図 2 1 のラウンド処理部の逆関数を持つラウンド処理部の構成例を示す図

【図 2 4】

同実施形態に係る暗号化装置のさらに他の構成例を示す図

【図 2 5】

図 2 4 の第 1 のユニット D U の構成例を示す図

【図 2 6】

図 2 4 の第 2 のユニット D D の構成例を示す図

【図 2 7】

図 2 4 の第 3 のユニット D D (w o M D S H) の構成例を示す図

【図 2 8】

図 2 4 の拡大鍵生成部の構成例を示す図

【図 2 9】

図 2 4 の拡大鍵生成部の他の構成例を示す図

【図 3 0】

図 2 8 と図 2 9 の非線形関数ユニットを説明するための図

【図 3 1】

図 2 8 と図 2 9 の排他的論理和によるユニットを説明するための図

【図 3 2】

図 2 8 と図 2 9 の排他的論理和によるユニットを説明するための図

【図 3 3】

図 2 8 と図 2 9 のガロア体上の乗算によるユニットを説明するための図

【図 3 4】

図 2 8 と図 2 9 のガロア体上の乗算によるユニットを説明するための図

【図 3 5】

同実施形態の暗号方式を利用したシステムの一例を示す図

【図 3 6】

同実施形態の暗号方式を利用したシステムの他の例を示す図

【図 3 7】

同実施形態の暗号方式を利用したシステムのさらに他の例を示す図

【図 3 8】

従来の拡大鍵生成装置について説明するための図

【図 3 9】

従来の拡大鍵生成装置について説明するための図

【符号の説明】

1, 2 …データ攪拌部

3, 4 …拡大鍵生成部

1 1, 1 2 …攪拌処理部

3 1, 4 2 …ラウンド処理部

3 3, 4 4 …拡大鍵変換部

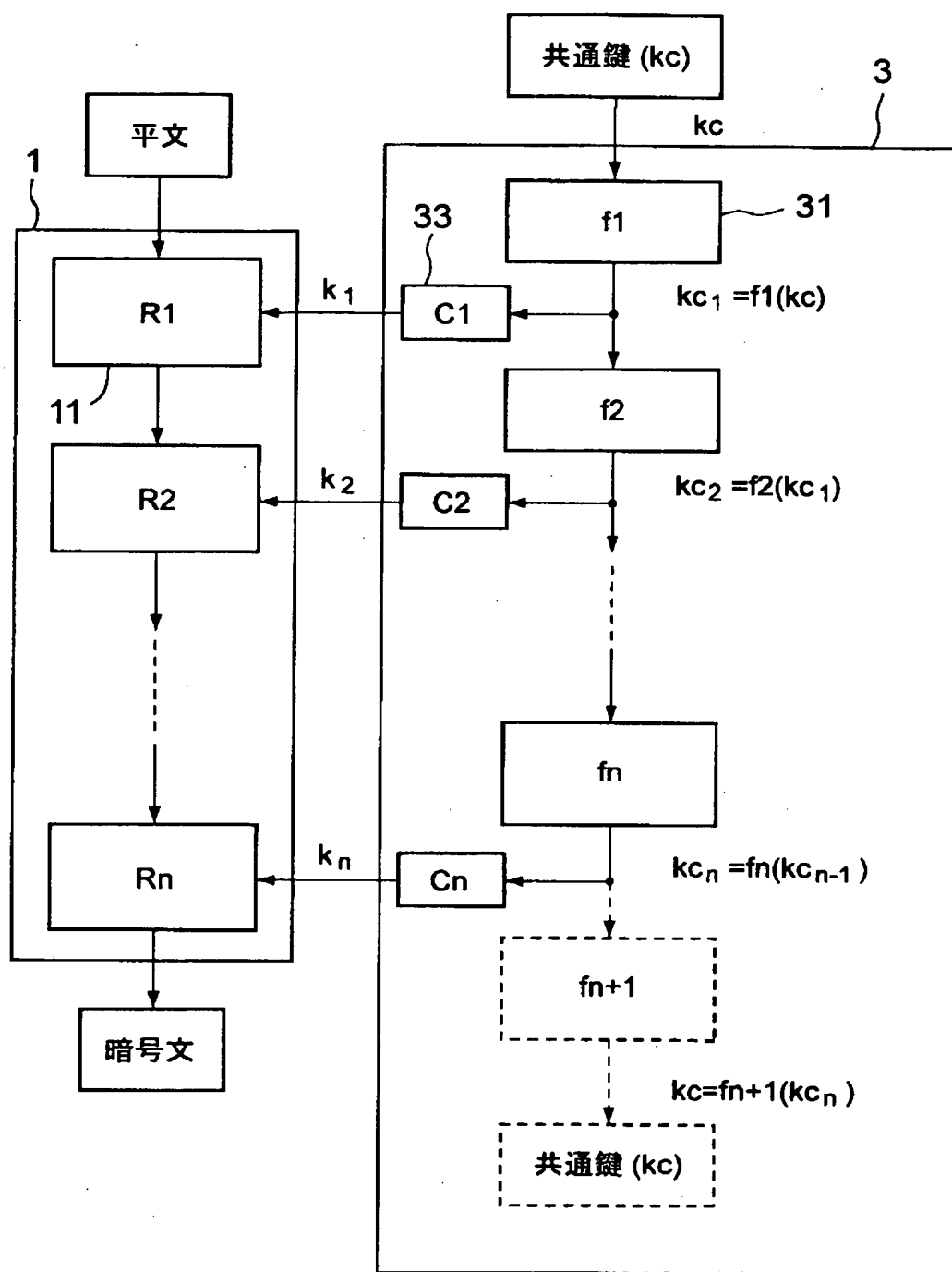
7, 8 …デコーダ

1 5, 1 6 …スイッチング回路

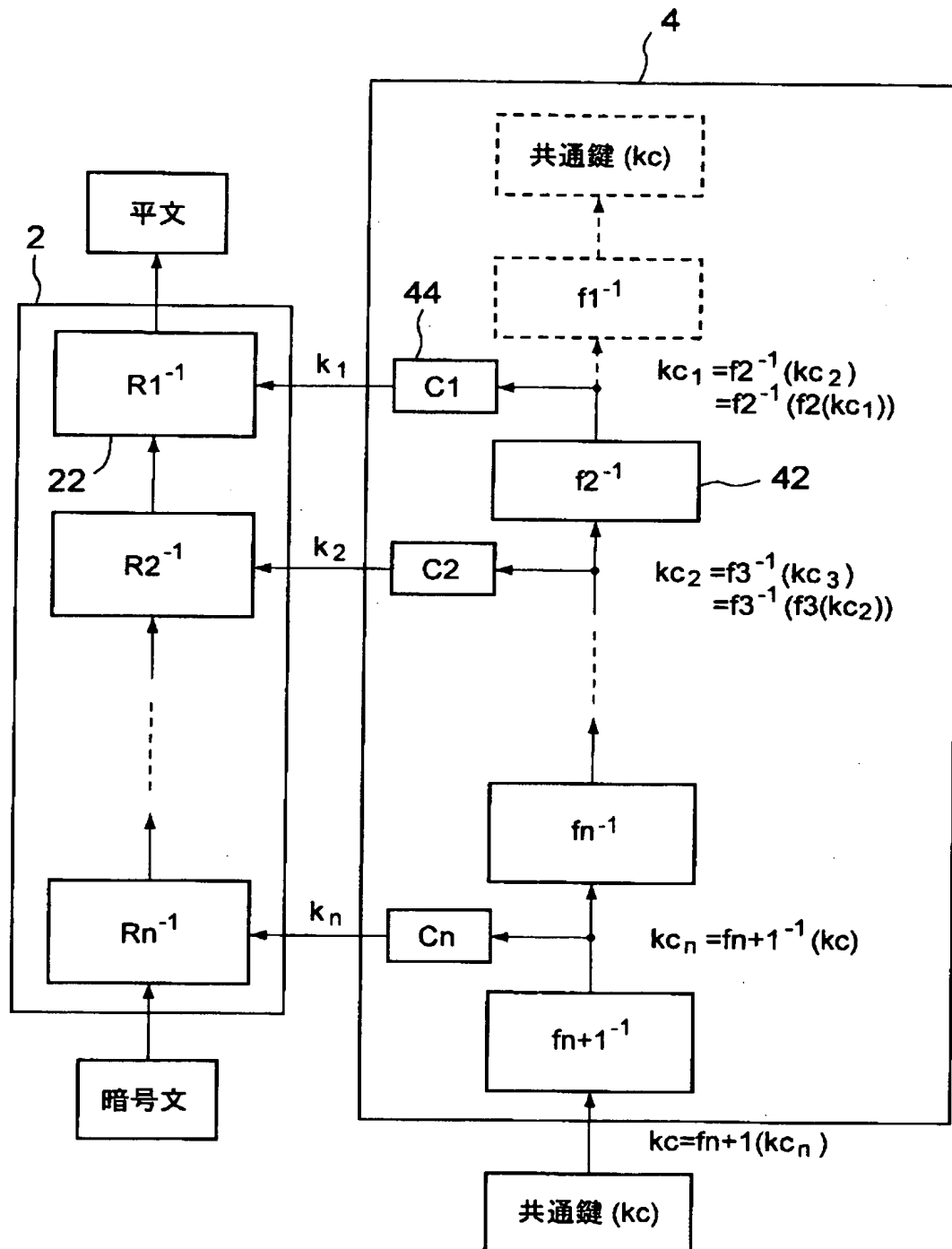
【書類名】

図面

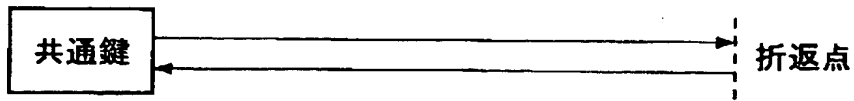
【図 1】



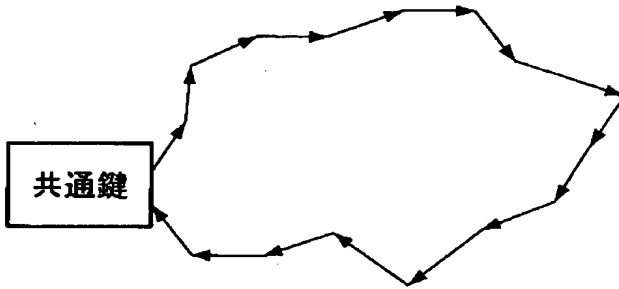
【図 2】



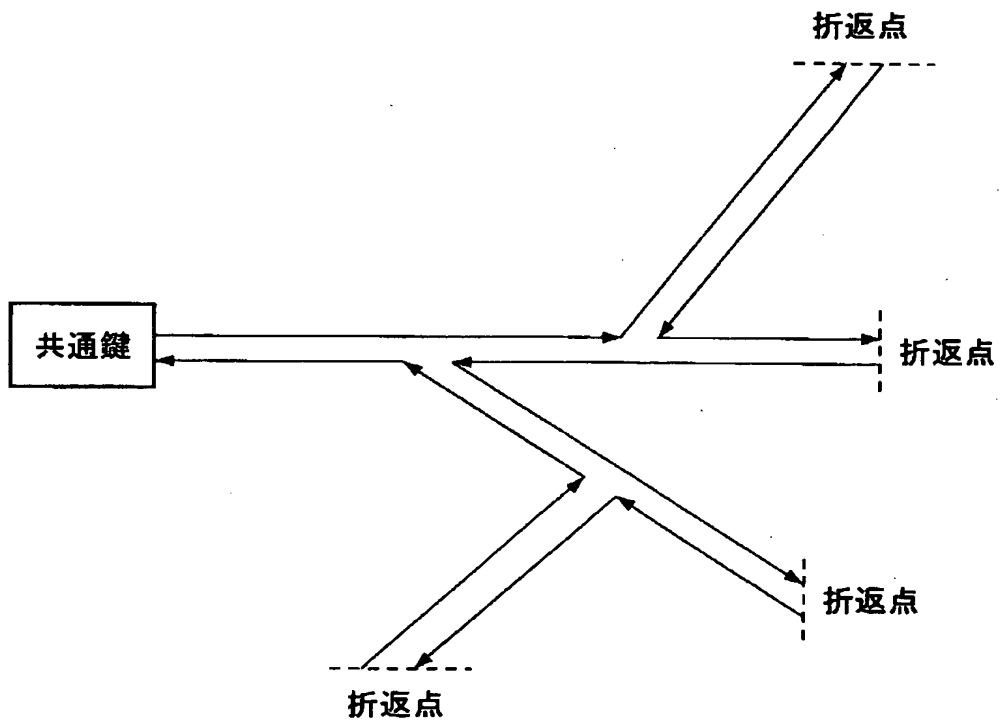
【図3】



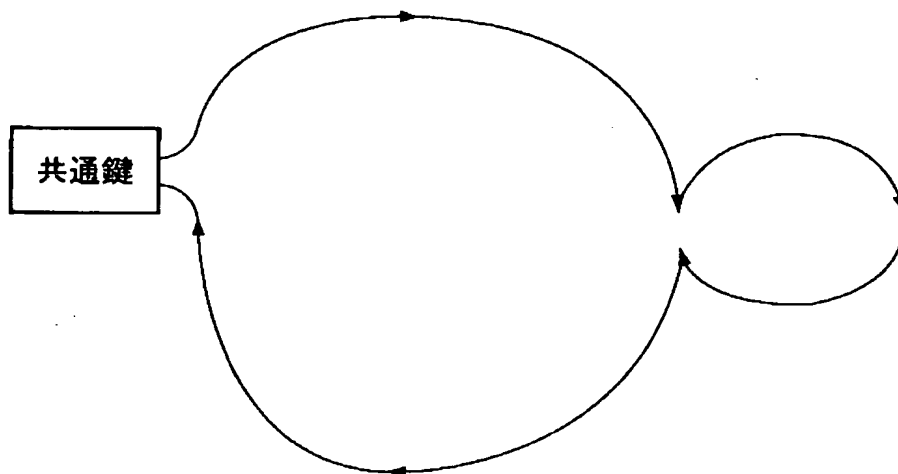
【図4】



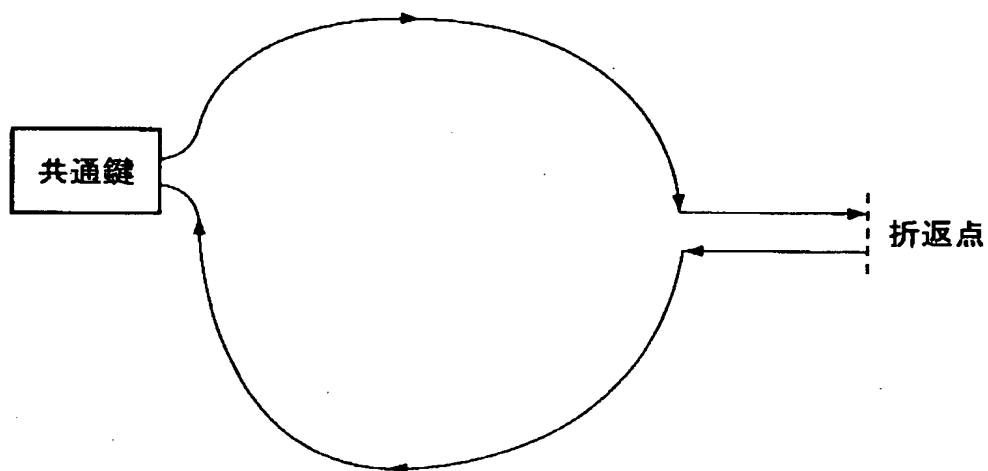
【図5】



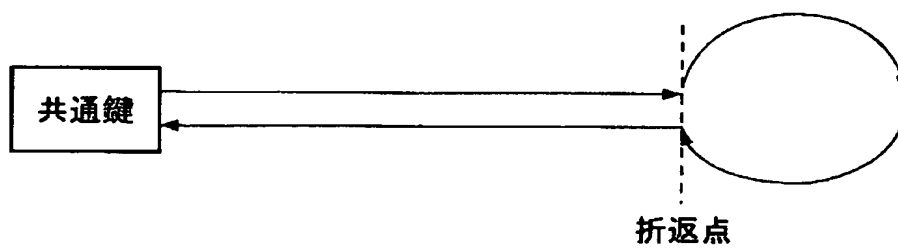
【図 6】



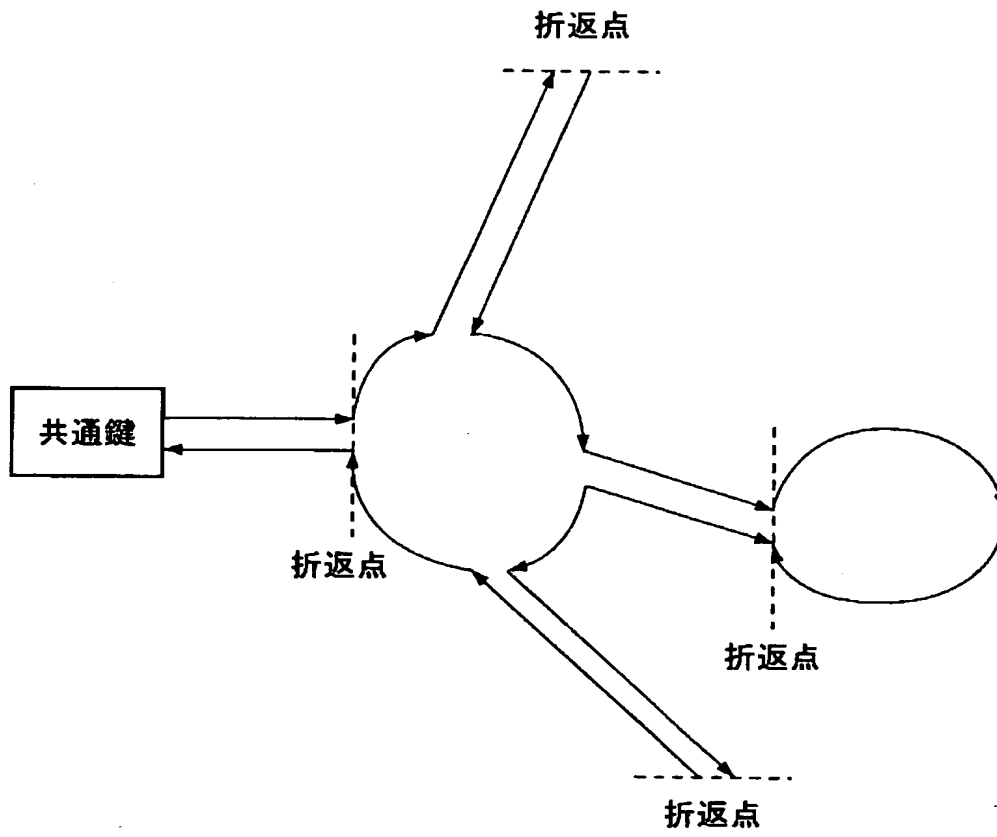
【図 7】



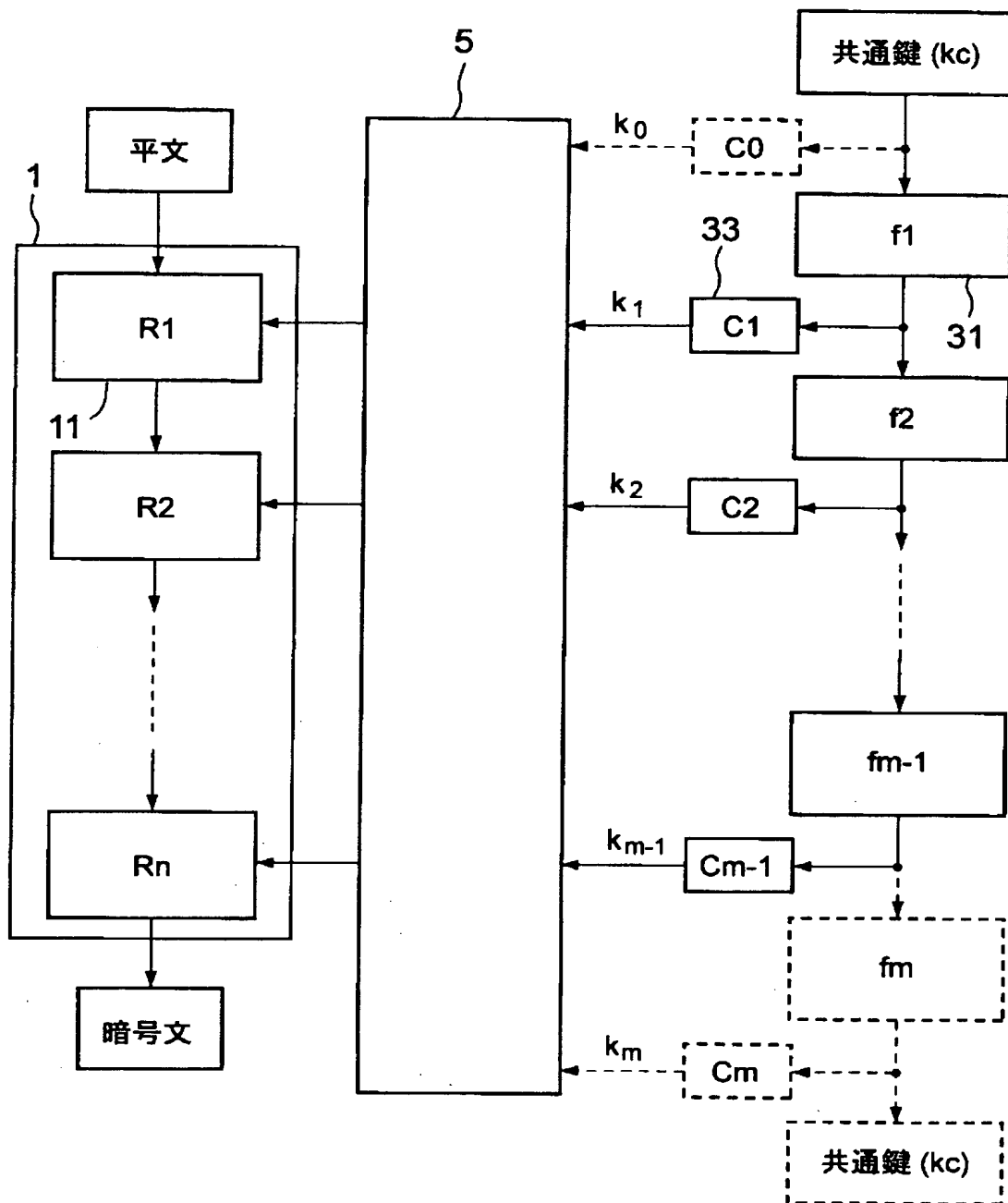
【図 8】



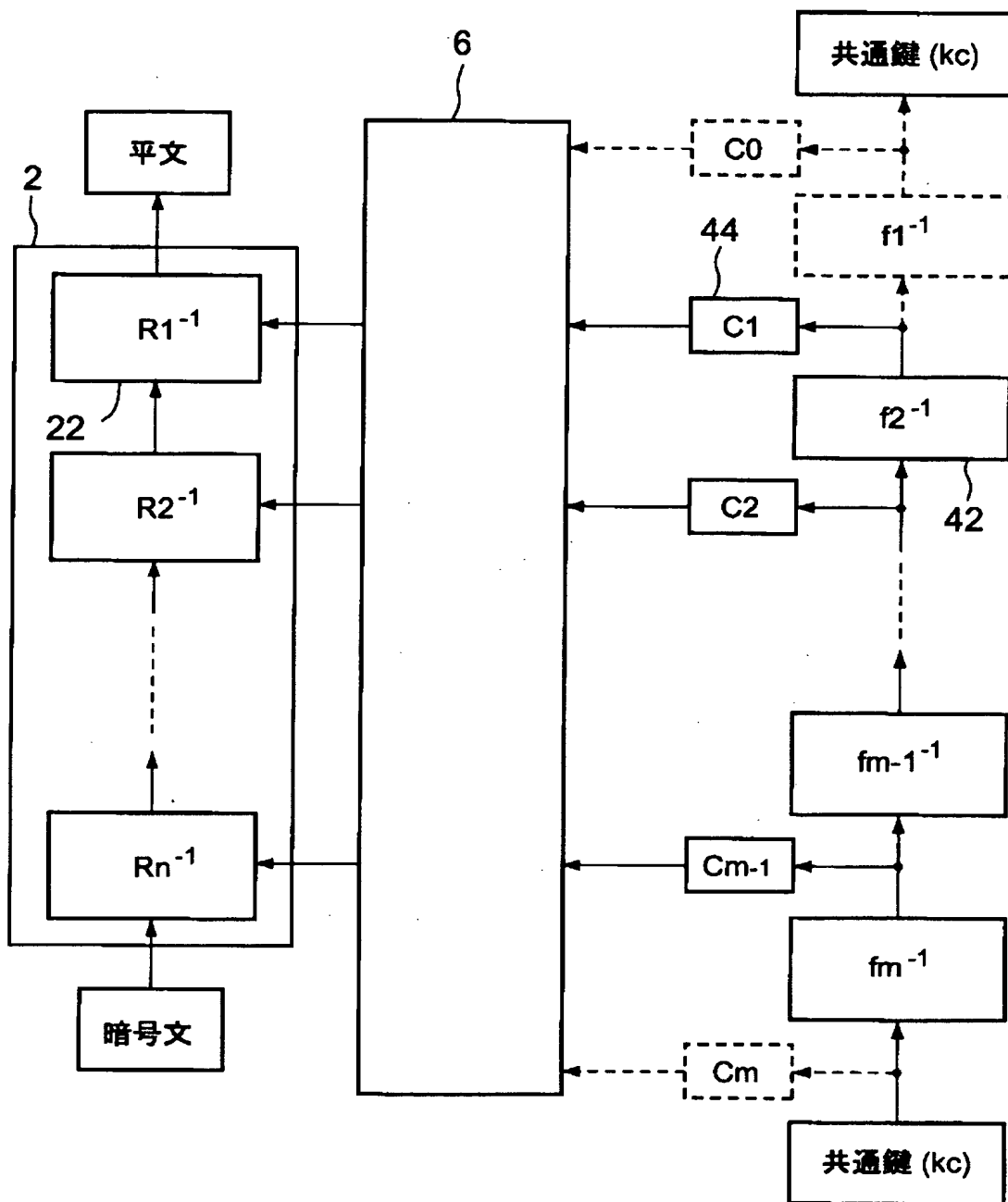
【図9】



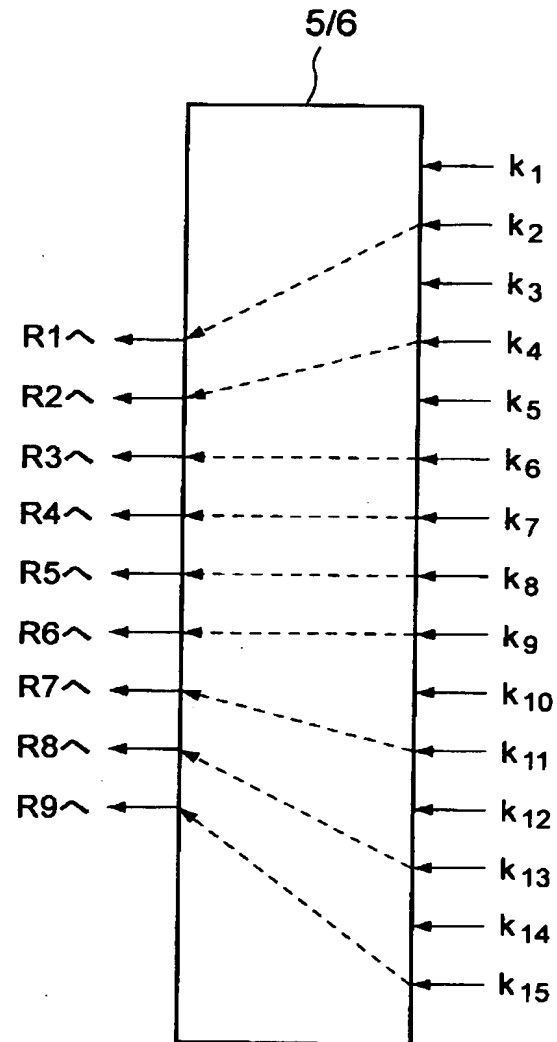
【図10】



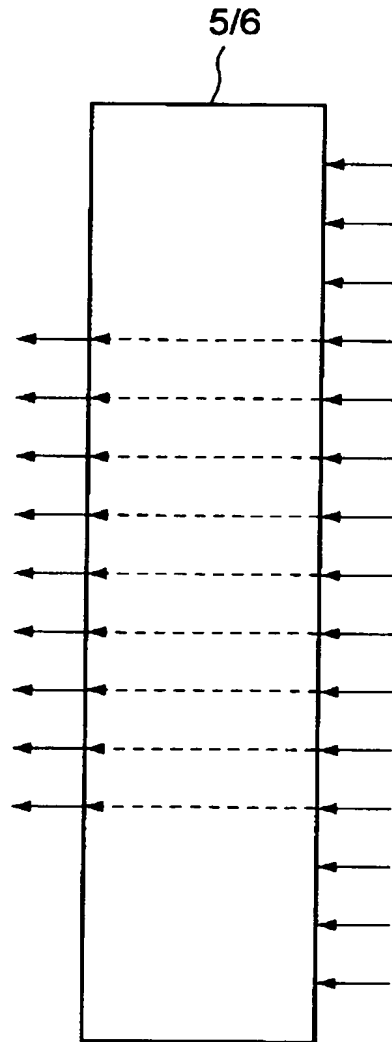
【図 11】



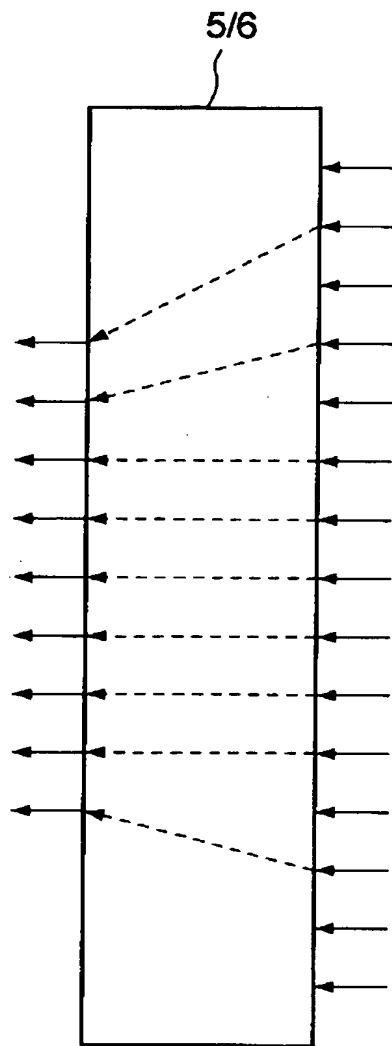
【図 1 2】



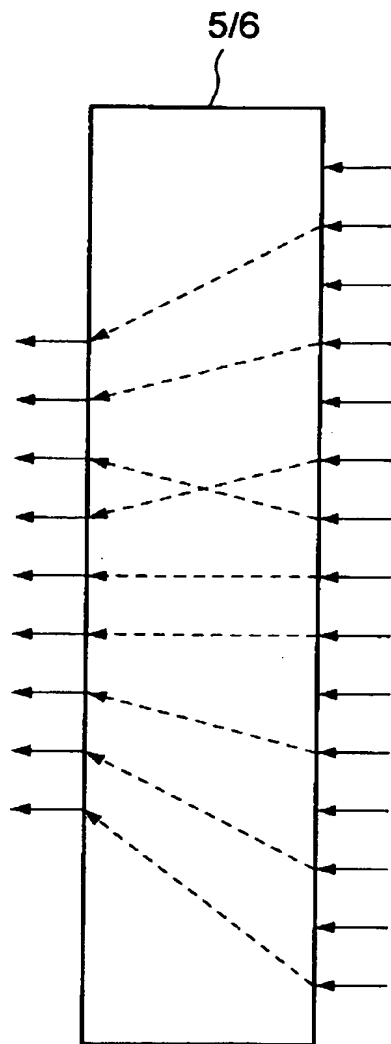
【図 1 3】



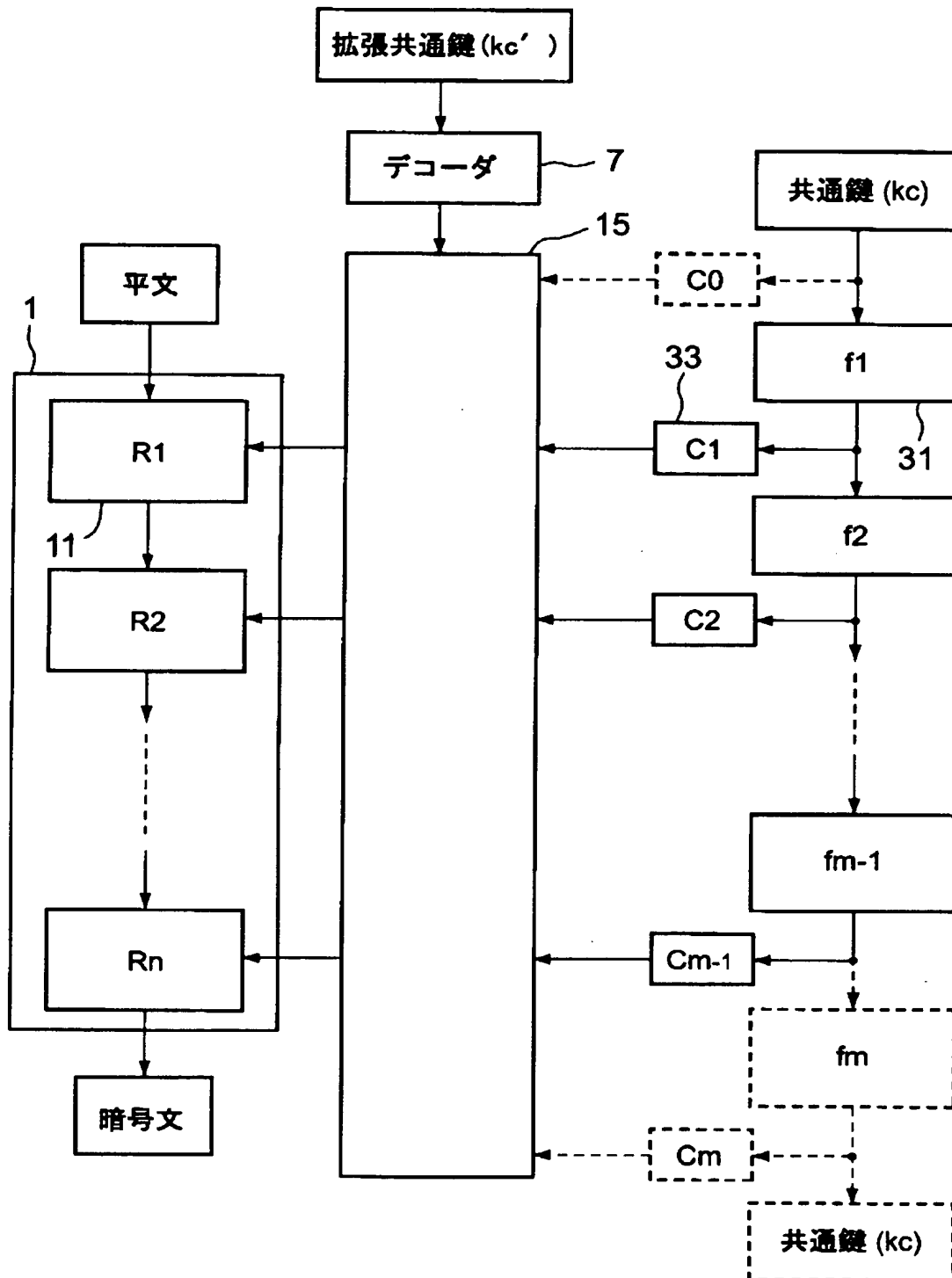
【図 1 4】



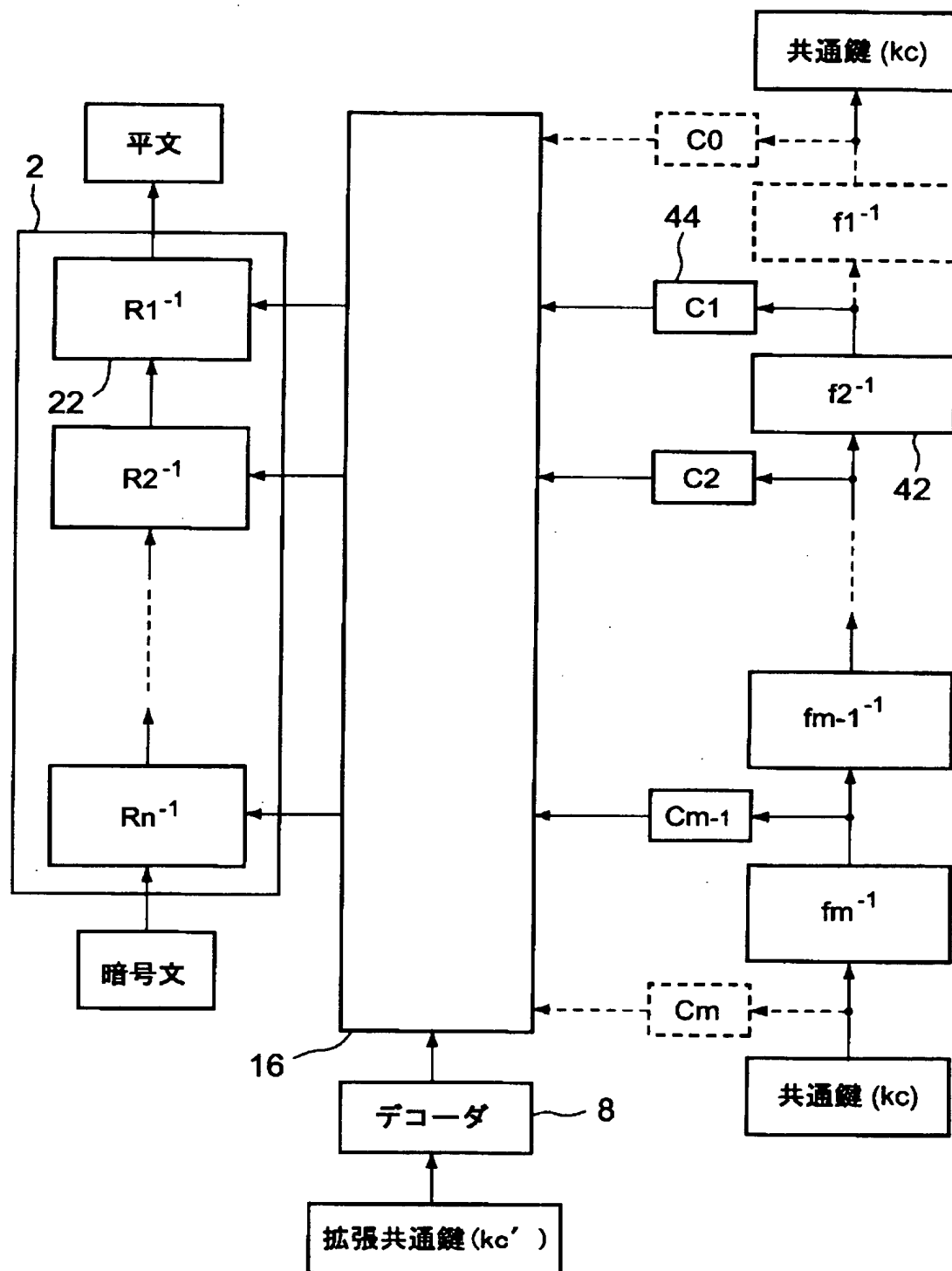
【図 1 5】



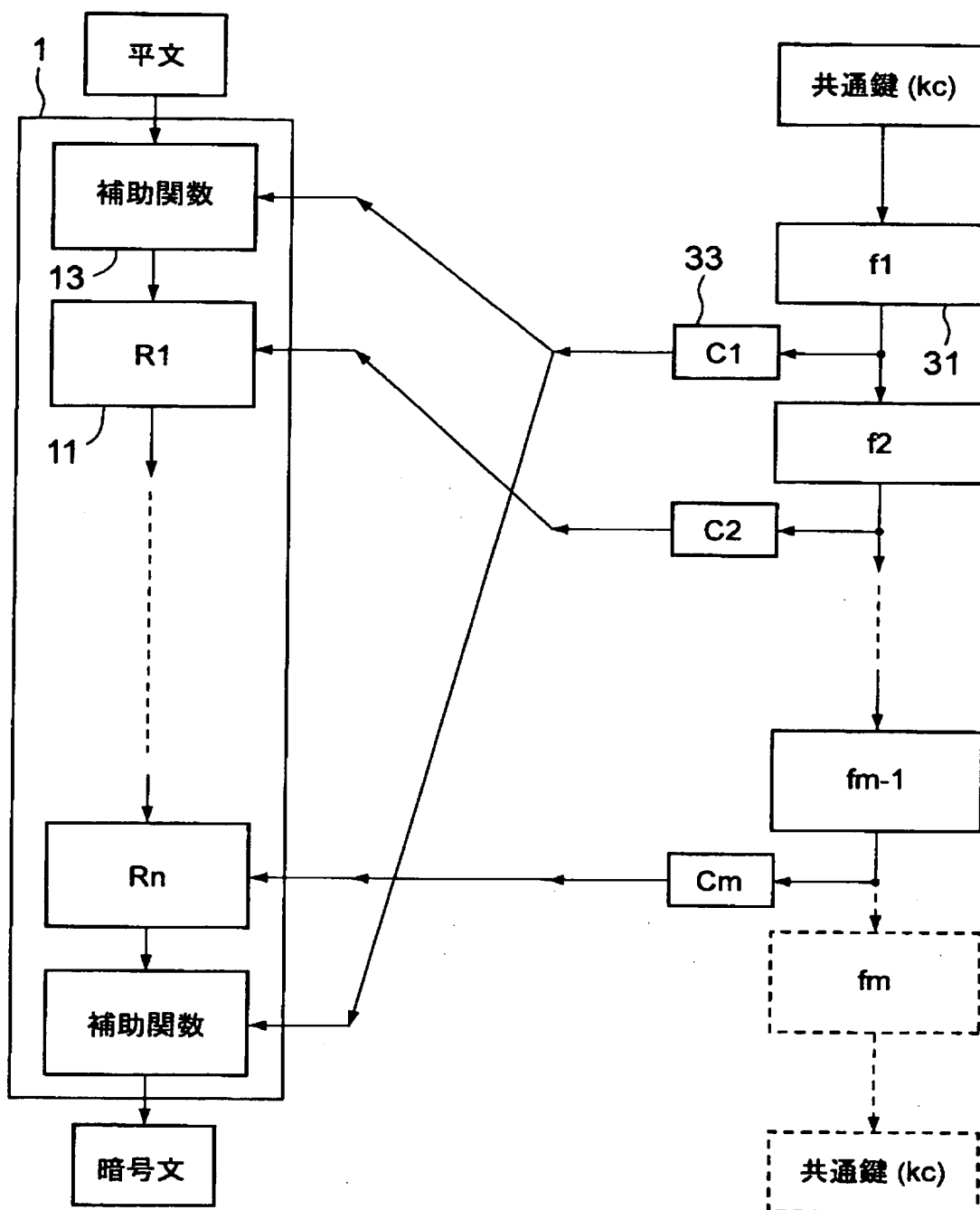
【図 16】



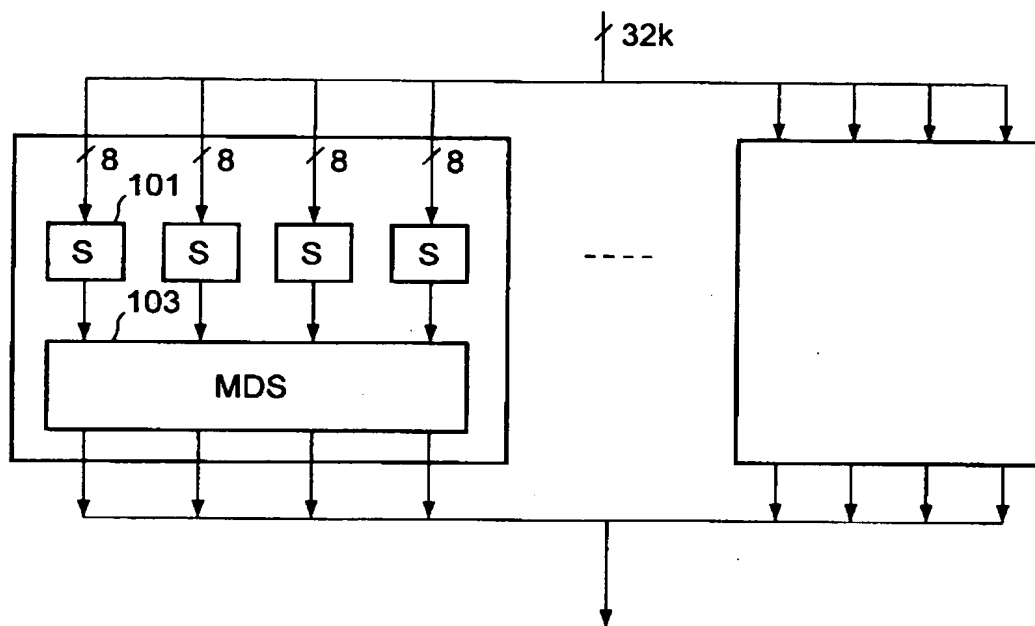
【図 17】



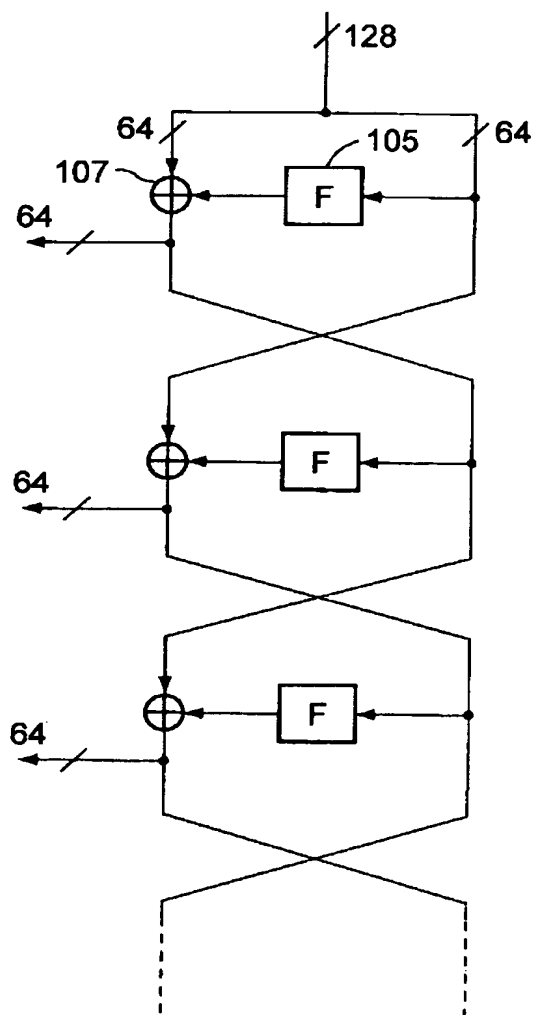
【図18】



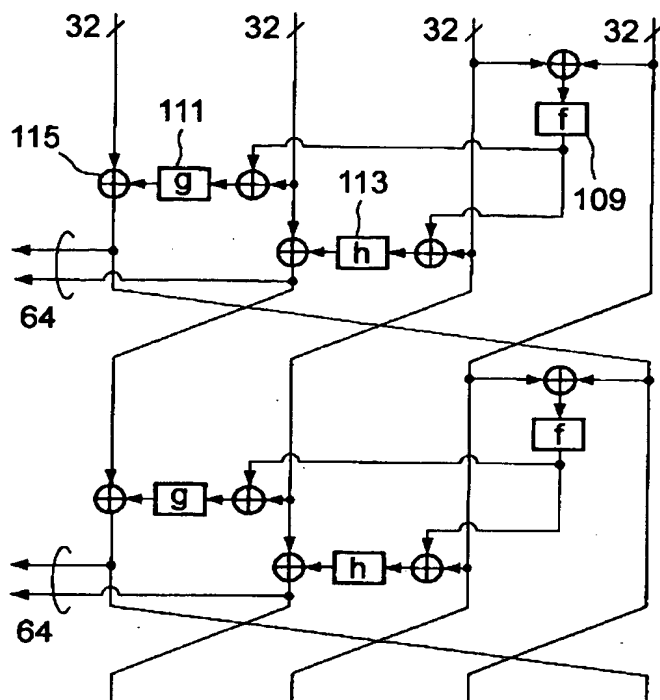
【図 1 9】



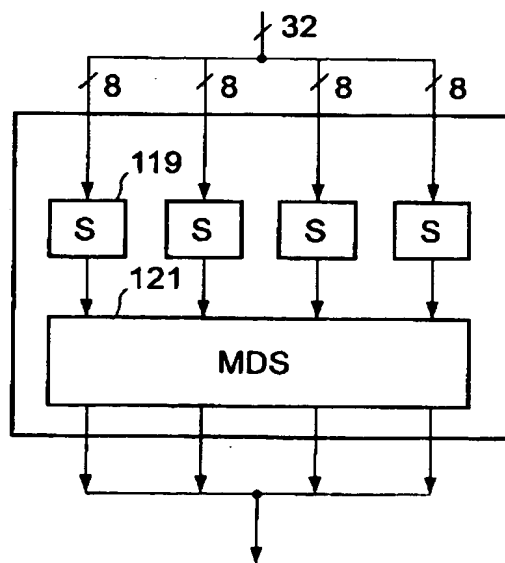
【図 2 0】



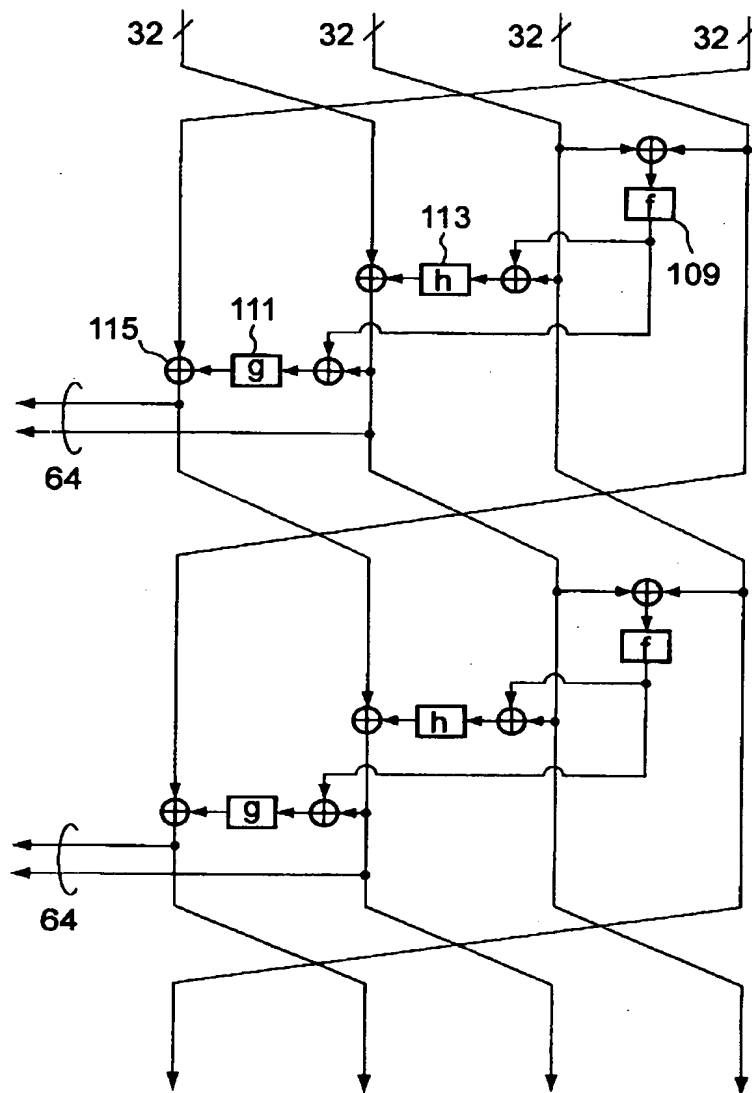
【図 2 1】



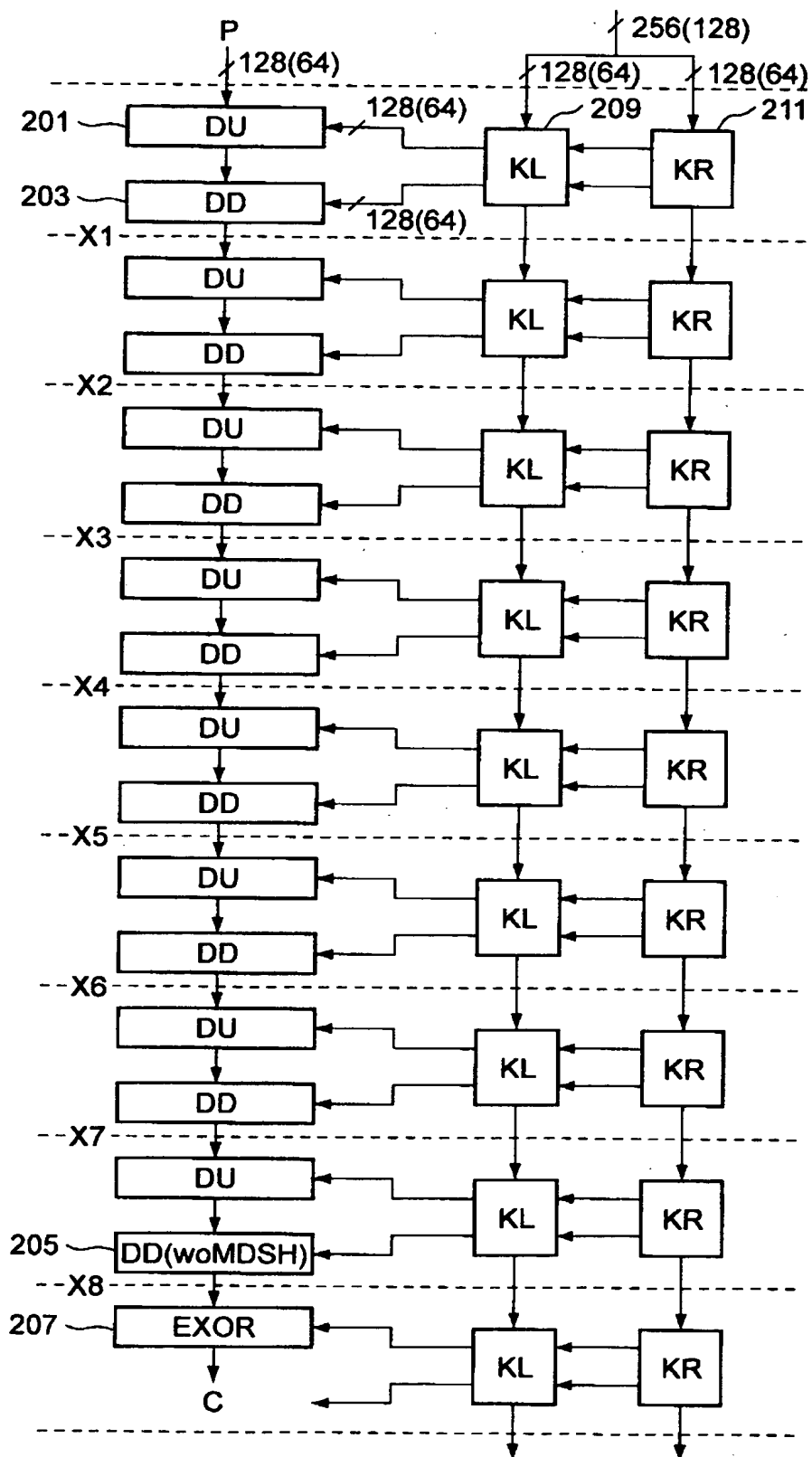
【図 2 2】



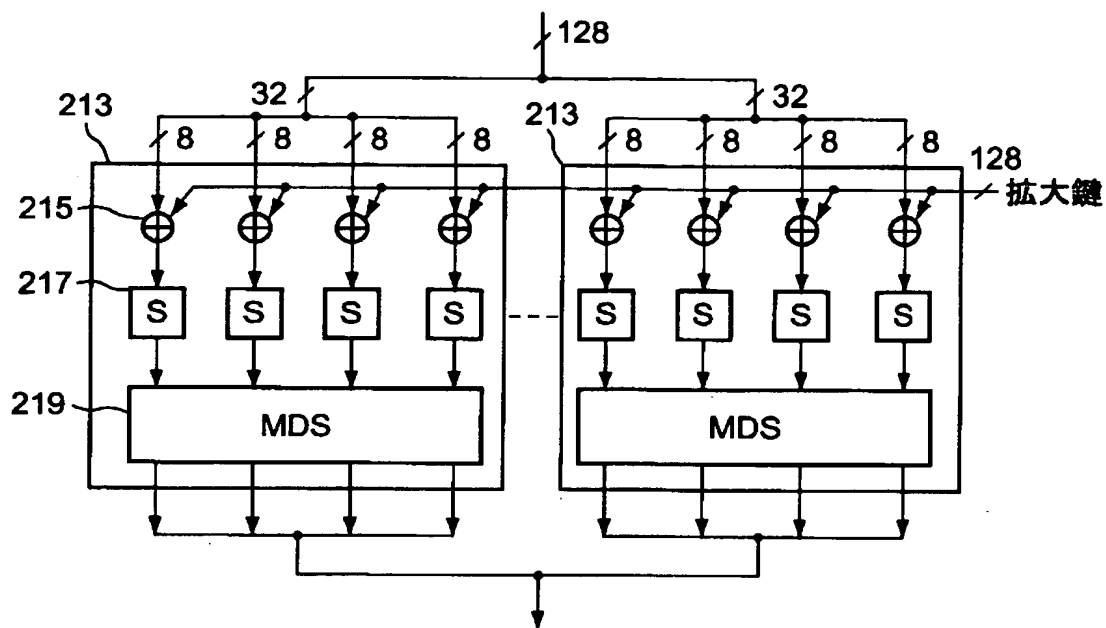
【図 2 3】



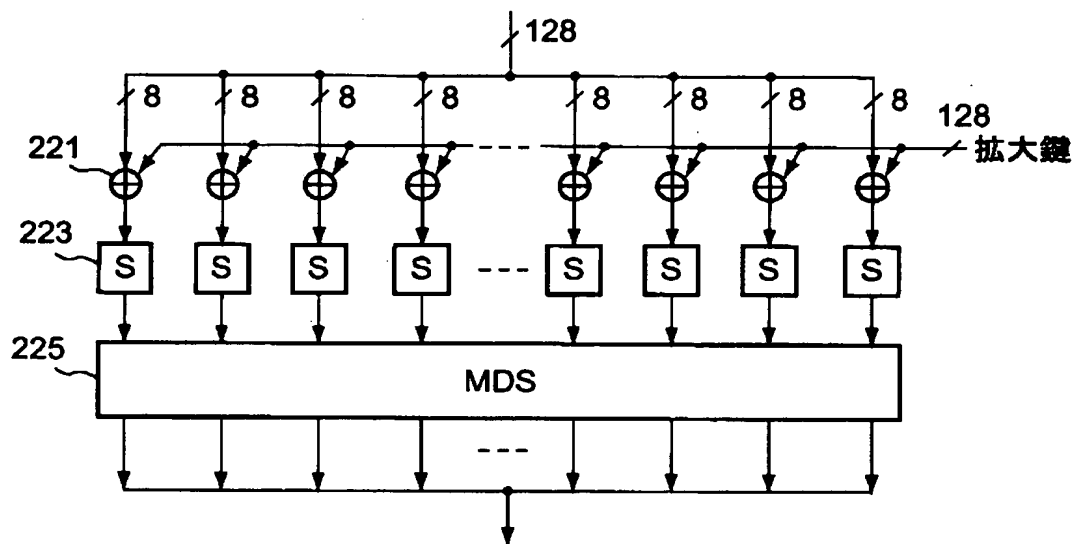
【図 24】



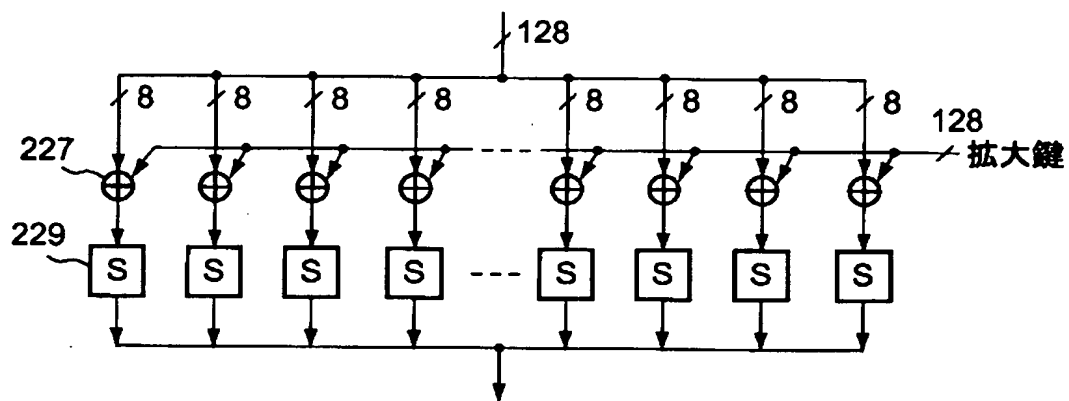
【図 2 5】



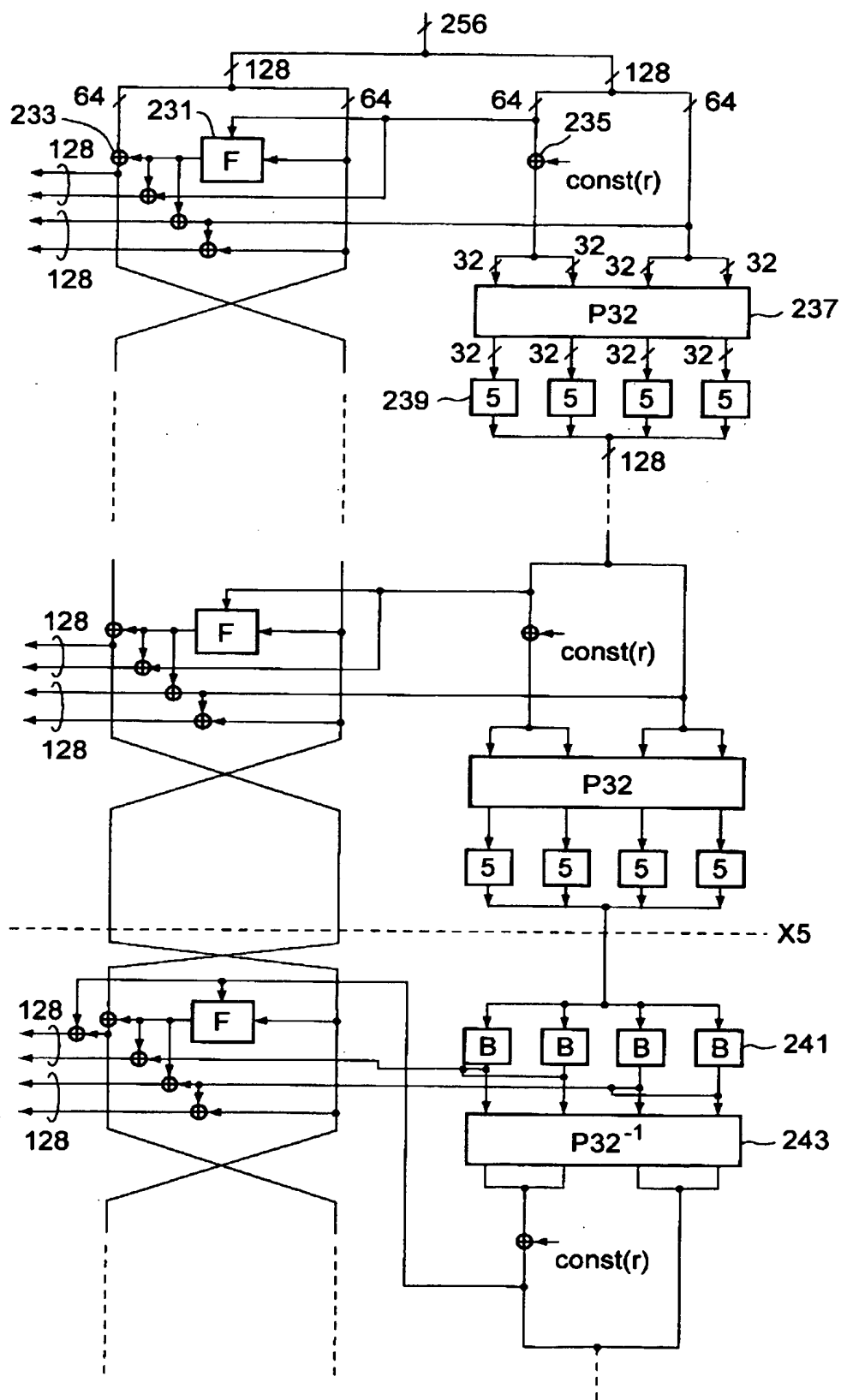
【図 2 6】



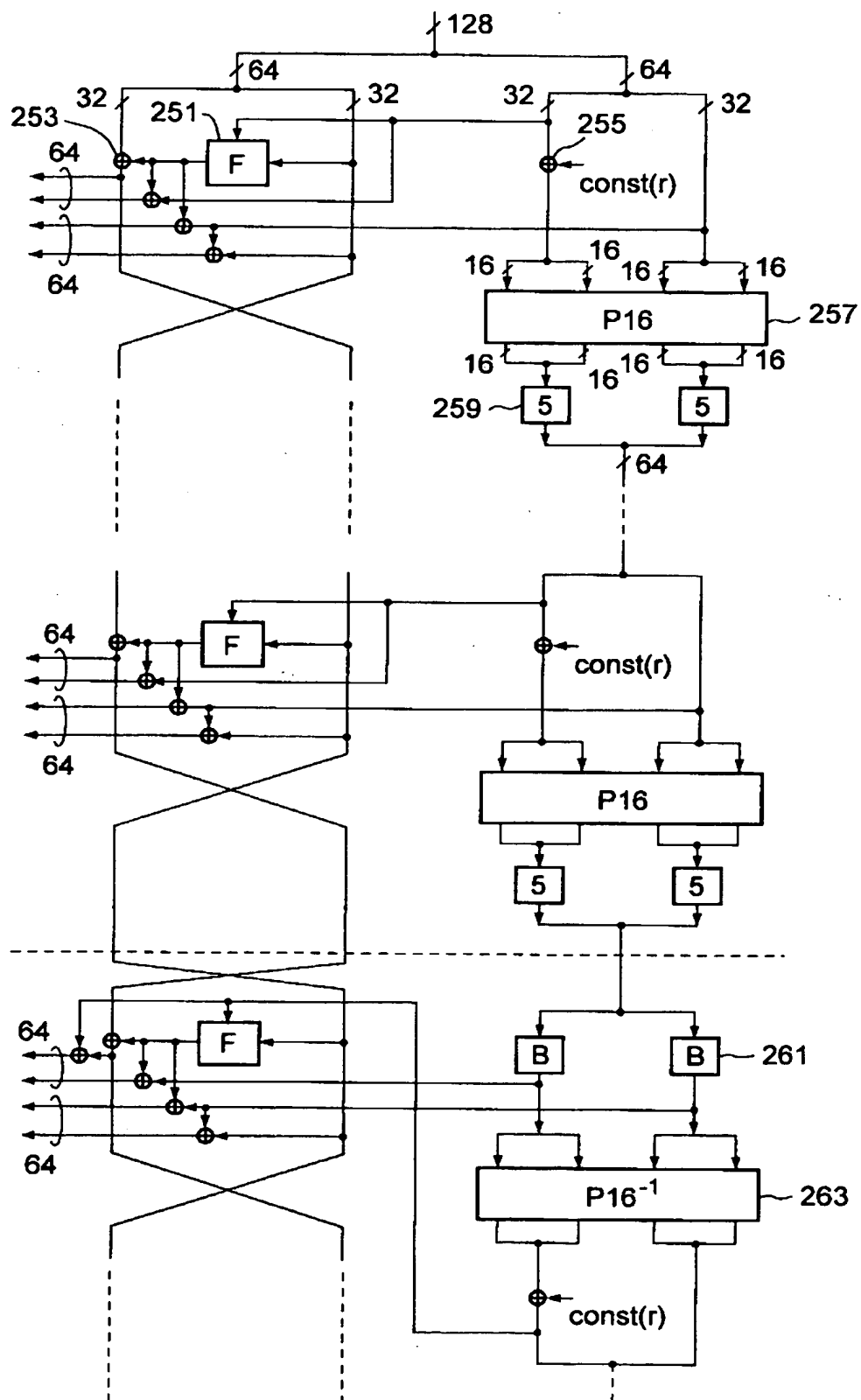
【図 2 7】



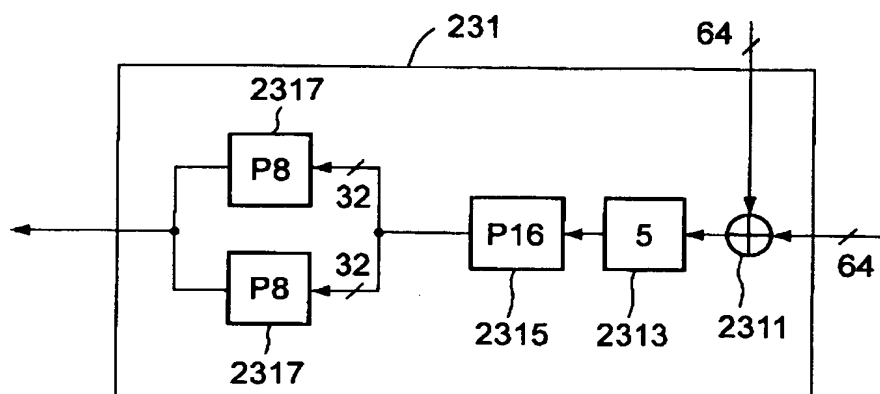
【図 28】



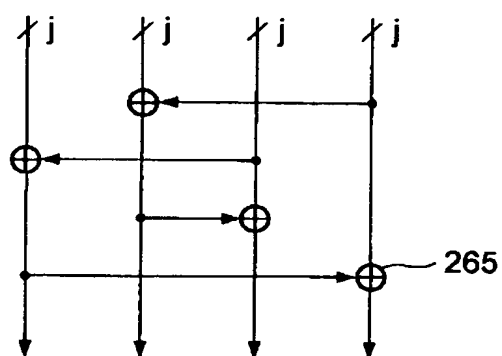
【図 2 9】



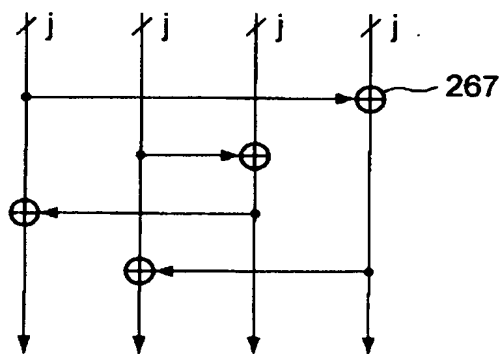
【図 3 0】



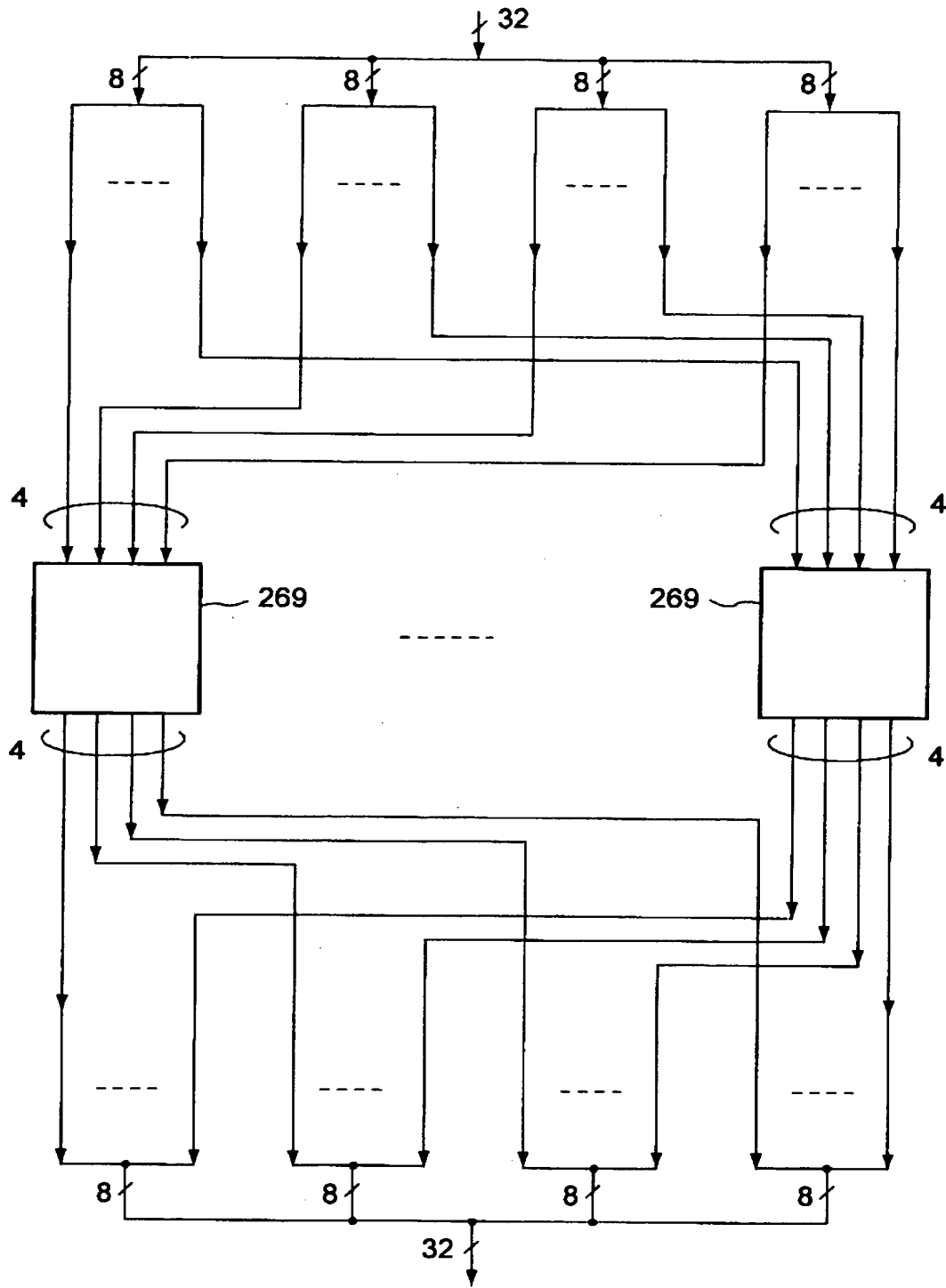
【図 3 1】



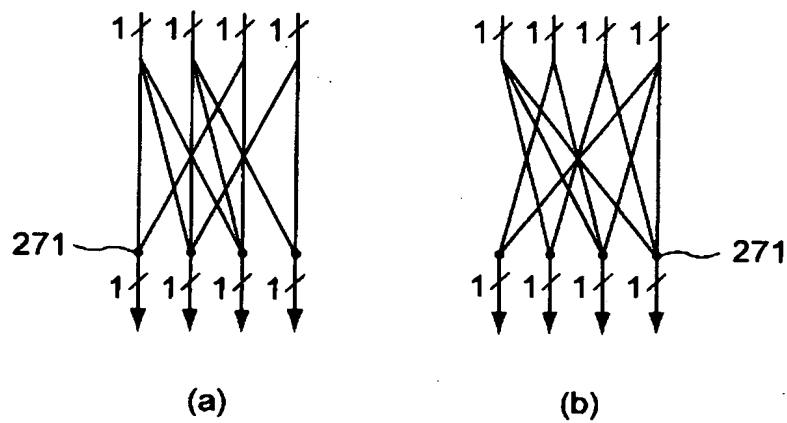
【図 3 2】



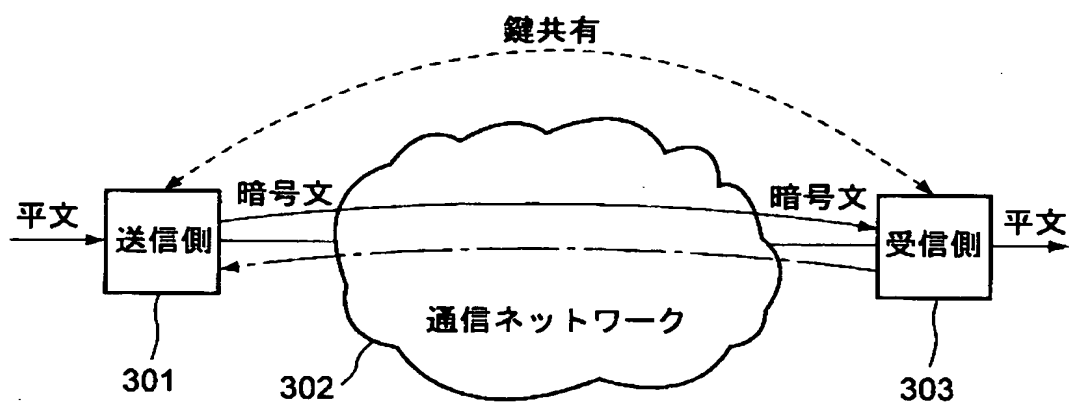
【図 33】



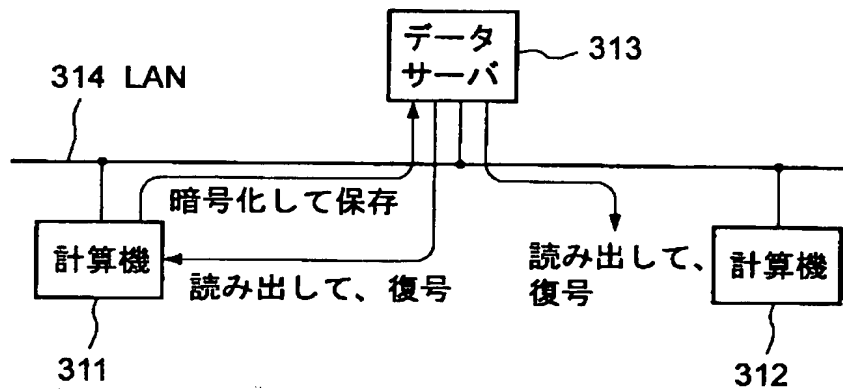
【図 3 4】



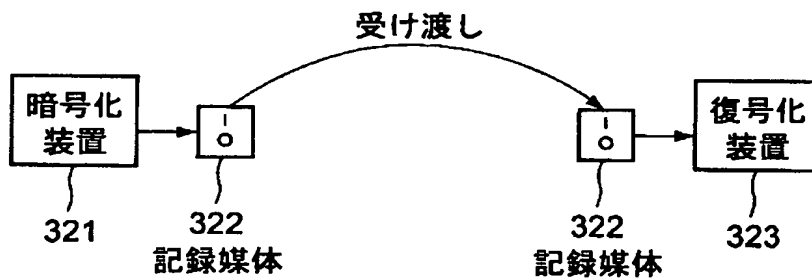
【図 3 5】



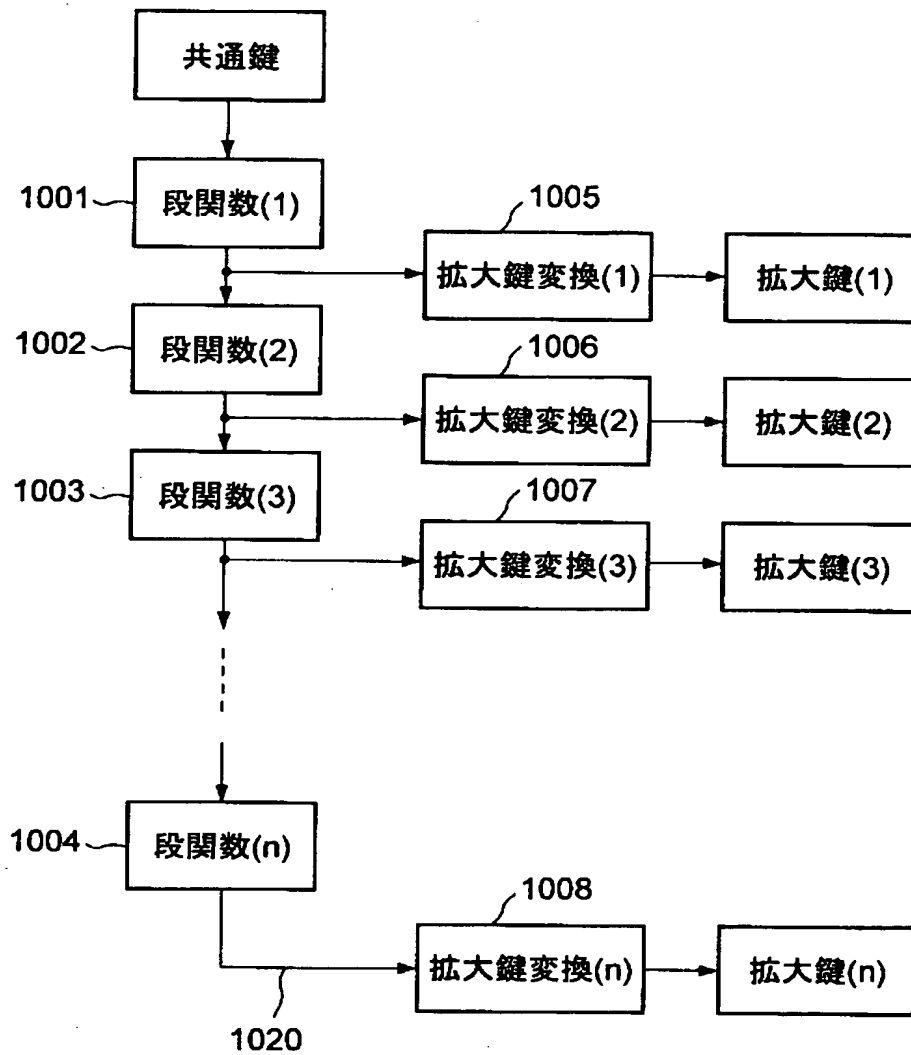
【図 3 6】



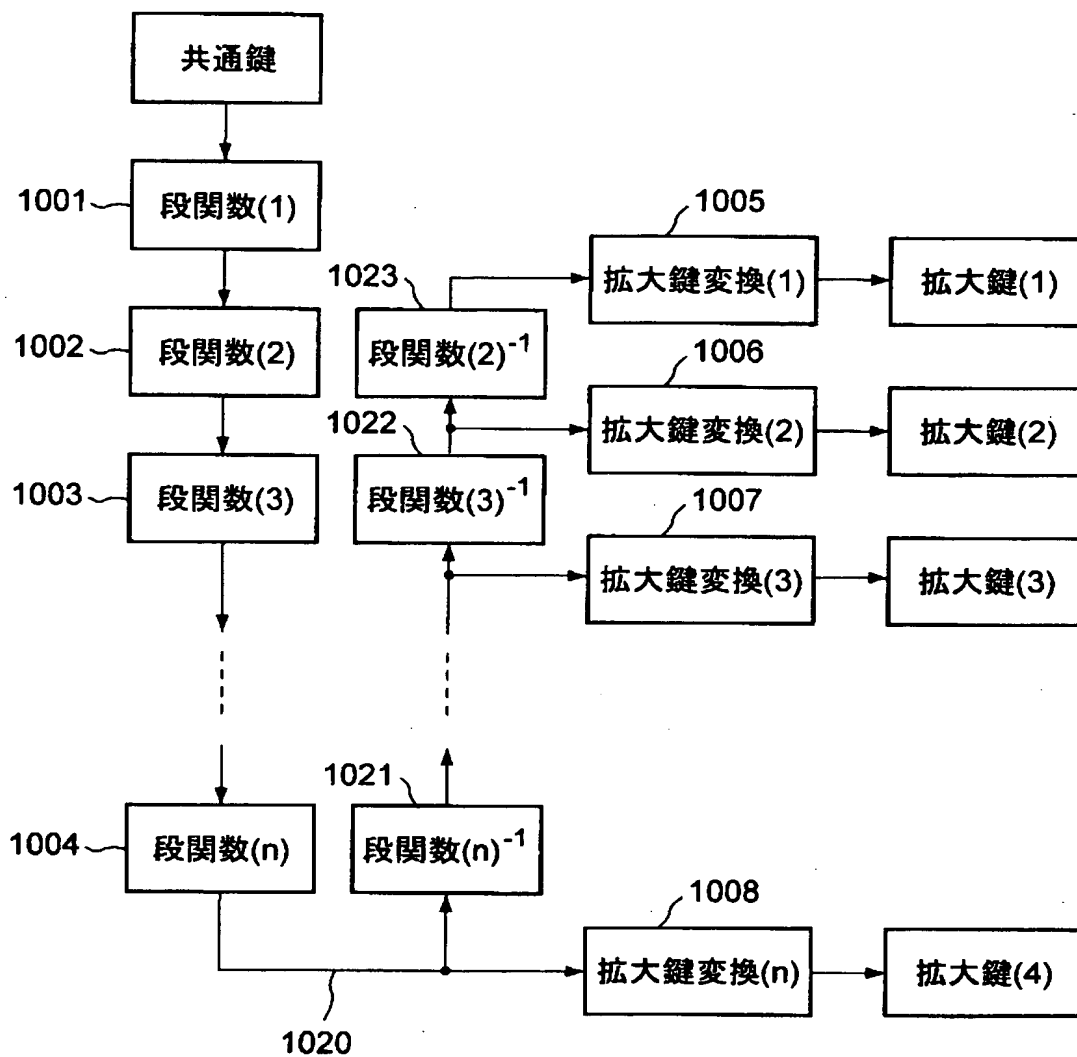
【図 3 7】



【図 3 8】



【図 3 9】



【書類名】 要約書

【要約】

【課題】 拡大鍵生成のための遅延時間の発生を回避し且つ $On-the-fly$ の鍵生成を可能とした暗号化装置を提供すること。

【解決手段】 暗号化時と復号時とで拡大鍵の使用順が逆になる共通鍵ブロック暗号方式の暗号化装置の拡大鍵生成部 3 において、初段からの段数と、最終段からの段数とが等しい 2 つのラウンド関数 f_1 と f_{n+1} とを、互いに逆関数になるように設定する。これによって、暗号化時にも復号時にも共通鍵を入力として直ちに且つ使用順に拡大鍵を逐次生成していくことが可能になる。また、暗号化時の拡大鍵生成と復号時の拡大鍵生成とが基本的に同一になる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝